

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-169048
(43)Date of publication of application : 13.06.2003

(51)Int.Cl. H04L 9/08
G11B 20/10
H04N 5/91

(21)Application number : 2002-089674 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 27.03.2002 (72)Inventor : NAKANO TOSHIHISA
OMORI MOTOJI
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO

(30)Priority

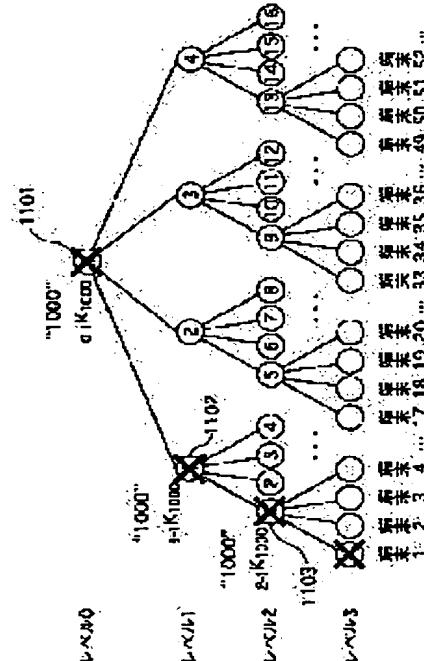
(54) DATA PROTECTION SYSTEM FOR PROTECTING DATA THROUGH ENCRYPTION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system which suppresses an increase in the amount of encryption data to be distributed to many terminals and encrypts data so that the data can not correctly be decrypted on a specified terminal.

SOLUTION: For individual nodes except for those in the bottom layer in a quadrant tree wherein terminals are made to correspond to respective bottom- layer nodes, a plurality of combination patterns as to four nodes in layers which are reached from the nodes and one layer below them are determined, individual keys are determined by the combination patterns, individual keys are determined by the respective nodes in the bottom layers, and each terminal stores and holds all keys determined as to individual nodes on the corresponding path from the bottom layer node to the top layer. The individual nodes on the path from the node corresponding to a specified terminal (terminal 1) to the top layer are defined as ineffective nodes (mark 'X' in

Fig. 15) and keys determined corresponding to the combination patterns of all nodes except ineffective nodes among four nodes of the layer which is reached from the ineffective nodes other than the bottom layer and one stage below the layer are specified and used to cipher data to be distributed.



LEGAL STATUS

Best Available Copy

This Page Blank (uspto)

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

This Page Blank (uspto)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2003-169048
(P2003-169048A)

(43)公開日 平成15年6月13日 (2003.6.13)

(51)Int.Cl.
H 04 L 9/08
G 11 B 20/10
H 04 N 5/91

識別記号

F I
G 11 B 20/10
H 04 L 9/00
H 04 N 5/91

テ-ヤコ-ト(参考)
H 5 C 05 3
6 0 1 B 5 D 0 4 4
P 5 J 1 0 4

審査請求 未請求 請求項の数41 O L (全 38 頁)

(21)出願番号 特願2002-89674(P2002-89674)
(22)出願日 平成14年3月27日 (2002.3.27)
(31)優先権主張番号 特願2001-95730(P2001-95730)
(32)優先日 平成13年3月29日 (2001.3.29)
(33)優先権主張国 日本 (JP)
(31)優先権主張番号 特願2001-285608(P2001-285608)
(32)優先日 平成13年9月19日 (2001.9.19)
(33)優先権主張国 日本 (JP)

(71)出願人 000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者 中野 稔久
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(72)発明者 大森 基司
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(74)代理人 100090446
弁理士 中島 司朗

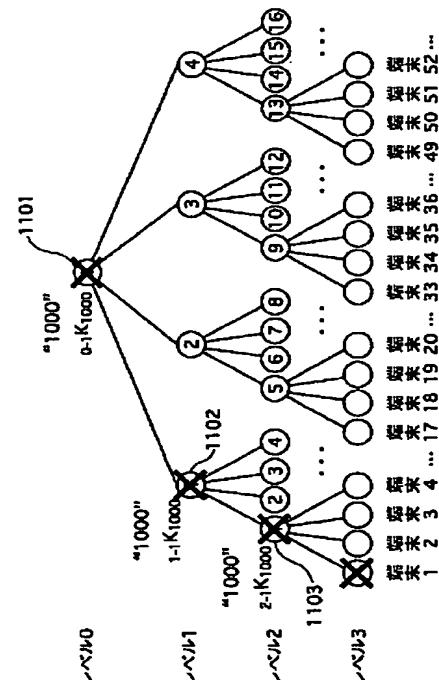
最終頁に続く

(54)【発明の名称】 暗号化を施すことによりデータを保護するデータ保護システム

(57)【要約】

【課題】 多数の端末に配給する暗号化データの量の増大化を抑制し、特定端末では正しく復号できないようにデータを暗号化するシステムを提供する。

【解決手段】 各端末を各最下層ノードに対応させた4分木の木構造で最下層を除く各ノードにつき、当該ノードから辿り着く1段下層の4個のノードについての複数の組合せパターンを決定し、組合せパターン毎に別個の鍵を定め、最下層の各ノード毎に別個の鍵を定め、各端末には対応する最下層ノードから最上層までの経路上の各ノードについて定めた全鍵を記憶保持させる。特定端末(端末1)に対応するノードから最上層への経路上の各ノードを無効ノード(図15中×印)と定め、最下層以外の各無効ノードにつき、当該ノードから辿り着く1段下層の4個のノードのうち無効ノードを除く全てのノードの組合せパターンに対応し定めている鍵を特定し、特定した各鍵を用いて配給用データを暗号化する。



【特許請求の範囲】

【請求項1】 3台以上の端末、暗号化装置及び暗号化鍵特定装置を備え、各端末への配給用データを暗号化装置により暗号化して保護するデータ保護システムであつて、

前記各端末は、所定鍵割当方法により個別に割当てられた復号鍵群を記憶しており、前記暗号化装置から出力された暗号化配給用データ群を取得して、暗号化配給用データを、記憶している復号鍵を用いて復号するものであり、

前記所定鍵割当方法は、

(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であつて、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

2つ以上の端末集合を決定し、

(b) 端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、

(c) 前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であり、

前記暗号化鍵特定装置は、暗号化鍵を特定する装置であり、かつ、

1つ以上の端末を無効化端末として特定する無効化端末特定手段と、

前記所定鍵割当方法により端末に割当てられた全ての復号鍵のうち無効化端末に割当てられた復号鍵以外の復号鍵を有効復号鍵と定めた場合において、

選定済みの有効復号鍵が割り当てられていない最も多くの端末に、割当てられている有効復号鍵を選定するという手順を、

選定済みの有効復号鍵が割り当てられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを有する装置であり、

前記暗号化装置は、前記暗号化鍵特定装置により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成して出力する暗号化手段を有することを特徴とするデータ保護システム。

【請求項2】 前記所定鍵割当方法は更に、前記複数の端末集合を完全に包含する端末集合が存在するように、かつ、同じ1つ以上の端末集合を各々包含する複数の端末集合であつて、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、端末集合の前記決

定を行う方法であることを特徴とする請求項1記載のデータ保護システム。

【請求項3】 前記所定鍵割当方法は更に、各端末集合が3台以上の端末を要素に含むように、かつ、3つ以上の端末集合を包含する端末集合が存在するように、端末集合の前記決定を行う方法であることを特徴とする請求項2記載のデータ保護システム。

【請求項4】 前記データ保護システムは、各端末を各々別個の最下位層のノードに対応させた複数

階層のN分木（Nは3以上の自然数）の木構造を想定した場合における最下位層を除く各ノードについて、当該ノード（親ノード）から辿り着く1段下位層のN個のノードのうち、2以上を組合せてなりN個全部の組合せを含む複数の組合せパターンを決定し、決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶しており、更に最下位層の各ノードに対応付けて別個の復号鍵を記憶している鍵記憶装置と、

前記所定鍵割当方法を実行し、前記各端末に割り当てる復号鍵群を決定する装置であり、かつ、

前記各端末について、当該端末に対応する最下位層のノードから最上位層のノードまでの経路上に位置する最下位層でない各ノードについて、当該ノードに対応付けて前記鍵記憶装置により記憶されている復号鍵のうち、当該ノードの1段下位層で当該経路上に位置するノードを含む組合せに係る全ての前記組合せパターンに対応する復号鍵と、当該端末に対応付けて前記鍵記憶装置により記憶されている復号鍵とを、当該端末に割り当てるべきものとして決定する復号鍵決定装置とを備え、

前記各端末集合は、前記各組合せパターンと一対一に対応し、対応する組合せパターンにおいて組み合わされた全ノードから辿り着く最下位層のノードに対応する全ての端末を要素とする集合に相当するものであり、前記暗号化鍵特定手段は、前記木構造を想定した場合において、いずれかの無効化端末に対応する最下位層のノードに辿り着く全てのノードを無効ノードと定め、まず最上位層ノードを処理対象ノードとしておき、未処理の処理対象ノードが存在しなくなるまで暗号化鍵特定処理を繰り返し行い、

前記暗号化鍵特定処理は、未処理の1つの処理対象ノードについて、

(a) 当該処理対象ノードの1段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在する場合には、当該組合せパターンに対応して前記鍵記憶装置により記憶されている復号鍵に呼応する暗号化鍵を特定し、

(b) 当該処理対象ノードの1段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在しない場合には、当該1段下位層が最下位層であれば当該1段下位層における無効ノード以外の全

てのノードに対応して前記鍵記憶装置により記憶されている復号鍵に呼応する暗号化鍵を特定し、当該1段下位層が最下位層でなければ当該1段下位層における無効ノード以外の全てのノードを新たに処理対象ノードとし、(c)当該処理対象ノードの1段下位層において無効ノードが存在すれば、当該1段階層が最下位層でない限り全ての無効ノードを新たに処理対象ノードとする処理であることを特徴とする請求項3記載のデータ保護システム。

【請求項5】 前記鍵記憶装置による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード(親ノード)から辿り着く1段下位層のN個のノードのうち、2以上を組合せてなる全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該鍵記憶装置は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード(親ノード)と対応付けて記憶していることを特徴とする請求項4記載のデータ保護システム。

【請求項6】 前記鍵記憶装置による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード(親ノード)から辿り着く1段下位層のN個のノードのうち、N個全部の組合せ及び(N-1)個の全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該鍵記憶装置は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード(親ノード)と対応付けて記憶していることを特徴とする請求項4記載のデータ保護システム。

【請求項7】 前記暗号化手段は、前記暗号化鍵特定装置により特定された全ての暗号化鍵それぞれについて、当該暗号化鍵を用いた暗号化により生成した暗号化配給用データと、前記鍵記憶装置により当該暗号化鍵に呼応する復号鍵と対応付けられていたノードの前記木構造における所在位置を特定するための暗号化鍵ノード識別情報を、対応付けて出力し、前記各端末は、所定鍵割当方法により個別に割当てられた各復号鍵を、前記鍵記憶装置により当該復号鍵と対応付けられていたノードの前記木構造における所在位置を特定するための復号鍵ノード識別情報を対応付けて記憶しており、前記暗号化装置から出力された暗号化配給用データ群及び暗号化鍵ノード識別情報群を取得して、当該端末が記憶している復号鍵ノード識別情報と一致する暗号化鍵ノード識別情報と対応する暗号化配給用データを、当該一致に係る復号鍵ノード識別情報と対応する復号鍵を用いて復号することを特徴とする請求項4記載のデータ保護システム。

【請求項8】 前記暗号化鍵特定装置は、前記鍵記憶装置により記憶されている各復号鍵に呼応する暗号化鍵を記憶している暗号化鍵記憶手段を有し、

前記呼応する復号鍵と暗号化鍵とは互いに異なることを特徴とする請求項4記載のデータ保護システム。

【請求項9】 前記暗号化手段による前記出力は、生成した前記暗号化配給用データ群をデータ記録媒体に記録することであり、

前記各端末は、前記暗号化装置により暗号化配給用データ群が記録されたデータ記録媒体から当該暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号することを特徴とする請求項1項記載のデータ保護

システム。

【請求項10】 前記暗号化手段は、デジタル著作物であるコンテンツデータを記憶しているコンテンツ記憶部と、乱数である前記配給用データを生成する乱数データ発生部と、

前記乱数データ発生部により生成された配給用データを鍵として用いて前記コンテンツデータを暗号化して、暗号化コンテンツデータを生成するコンテンツ暗号化部とを有し、

前記暗号化手段は、前記暗号化鍵特定装置により特定された全ての暗号化鍵を逐次用いて前記乱数データ発生部により生成された配給用データを暗号化することにより、暗号化配給用データ群を生成して、当該暗号化配給用データ群と、前記コンテンツ暗号化部により生成された暗号化コンテンツデータとを前記データ記録媒体に記録し、

前記各端末は、前記データ記録媒体から暗号化コンテンツデータ及び暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号し、復号結果である配給用データを用いて、当該暗号化コンテンツデータを復号することを特徴とする請求項9記載のデータ保護システム。

【請求項11】 前記データ保護システムは更に、前記暗号化鍵特定装置により特定された暗号化鍵を特定するための暗号化鍵特定情報を、データ記録媒体に記録する暗号化鍵特定情報記録装置を備え、

前記各端末は、乱数である前記配給用データを生成する乱数データ発生部と、

デジタル著作物であるコンテンツデータを格納しているコンテンツ格納部と、

前記データ記録媒体から暗号化鍵特定情報を読み出し、当該端末に記憶されている復号鍵群に呼応する暗号化鍵群のうち当該暗号化鍵特定情報で特定される暗号化鍵を選定する暗号化鍵選定部とを有し、

前記暗号化手段は、前記暗号化鍵選定部により選定された全ての暗号化鍵を逐次用いて前記乱数データ発生部により生成された配給用データを暗号化することにより暗号化配給用データ群を生成して、前記データ記録媒体に記録するものであり、

前記各端末は更に、

前記乱数データ発生部により生成された配給用データを鍵として用いて前記コンテンツ格納部に格納されているコンテンツデータを暗号化して、暗号化コンテンツデータを生成し、当該暗号化コンテンツデータを前記データ記録媒体に記録するコンテンツ暗号化部と、
前記各端末は、前記データ記録媒体から暗号化コンテンツデータ及び暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号し、復号結果である配給用データを用いて、当該暗号化コンテンツデータを復号することを特徴とする請求項9記載のデータ保護システム。

【請求項12】 前記暗号化手段による前記出力は、生成した前記暗号化配給用データ群を前記各端末に送信することであり、前記各端末は、前記暗号化装置により送信された暗号化配給用データ群を受信して取得し、暗号化配給用データを復号することを特徴とする請求項1記載のデータ保護システム。

【請求項13】 暗号化されたデータを取得して復号するための3台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定装置であって、

(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

2つ以上の端末集合を決定し、

(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、

前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当手段とを備えることを特徴とする復号鍵決定装置。

【請求項14】 前記復号鍵設定手段は更に、前記複数の端末集合を完全に包含する端末集合が存在するように、かつ、同じ1つ以上の端末集合を各々包含する複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、端末集合の前記決定を行うことを特徴とする請求項13記載の復号鍵決定装置。

【請求項15】 前記復号鍵設定手段は更に、各端末集合が3台以上の端末を要素に含むように、かつ、3つ以上の端末集合を包含する端末集合が存在するように、端

10

20

30

40

50

末集合の前記決定を行うことを特徴とする請求項14記載の復号鍵決定装置。

【請求項16】 前記復号鍵設定手段は、各端末を各々別個の最下位層のノードに対応させた複数階層のN分木（Nは3以上の自然数）の木構造を想定した場合における最下位層を除く各ノードについて、当該ノード（親ノード）から辿り着く1段下位層のN個のノードのうち、2以上を組合せてなりN個全部の組合せを含む複数の組合せパターンを決定し、決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶しており、更に最下位層の各ノードに対応付けて別個の復号鍵を記憶しており、

前記復号鍵群割当手段は、

前記各端末について、当該端末に対応する最下位層のノードから最上位層のノードまでの経路上に位置する最下位層でない各ノードについて、当該ノードに対応付けて前記復号鍵設定手段により記憶されている復号鍵のうち、当該ノードの1段下位層で当該経路上に位置するノードを含む組合せに係る全ての前記組合せパターンに対応する復号鍵と、当該端末に対応付けて前記復号鍵設定手段により記憶されている復号鍵とを、当該端末に割り当てるべきものとして決定し、

前記各端末集合は、

前記各組合せパターンと一対一に対応し、対応する組合せパターンにおいて組み合わされた全ノードからから辿り着く最下位層のノードに対応する全ての端末を要素とする集合に相当することを特徴とする請求項15記載の復号鍵決定装置。

【請求項17】 前記復号鍵設定手段による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く1段下位層のN個のノードのうち、2以上を組合せてなる全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該復号鍵設定手段は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることを特徴とする請求項16記載の復号鍵決定装置。

【請求項18】 前記復号鍵設定手段による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く1段下位層のN個のノードのうち、N個全部の組合せ及び（N-1）個の全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該復号鍵設定手段は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることを特徴とする請求項16記載の復号鍵決定装置。

【請求項19】 暗号化されたデータを取得して復号するための3台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定方法であつて、

前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であつて、当該複数の端末集合におけるいずれの1の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

2つ以上の端末集合を決定する端末集合決定ステップと、

端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当ステップとを含むことを特徴とする復号鍵決定方法。

【請求項20】 暗号化されたデータを取得して復号するための3台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定処理をコンピュータに実行させるためのコンピュータプログラムにおいて、

前記復号鍵決定処理は、

前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であつて、当該複数の端末集合におけるいずれの1の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

2つ以上の端末集合を決定する端末集合決定ステップと、

端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、

前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当ステップとを含むことを特徴とするコンピュータプログラム。

【請求項21】 暗号化されたデータを取得して復号するための3台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定処理をコンピュータに実行させるためのコンピュータプログラム

を記録した記録媒体において、

前記復号鍵決定処理は、

前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であつて、当該複数の端末集合におけるいずれの1の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

10 2つ以上の端末集合を決定する端末集合決定ステップと、

端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、

前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当ステップとを含むことを特徴とする記録媒体。

20 【請求項22】 暗号化されたデータを取得して復号するための3台以上の端末から構成される復号端末システムであつて、

前記各端末は、

所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、

暗号化されたデータを取得する暗号化データ取得手段と、

前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて

30 復号する復号手段とを備え、

前記所定鍵割当方法は、

(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、

更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であつて、当該複数の端末集合におけるいずれの1の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

2つ以上の端末集合を決定し、

40 (b) 端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、

(c) 前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする復号端末システム。

【請求項23】 前記暗号化データ取得手段は、前記暗号化されたデータをデータ記録媒体から読み出して取得することを特徴とする請求項22記載の復号端末システム。

50 【請求項24】 前記データ記録媒体には、暗号化鍵を

特定するための暗号化鍵特定情報が記録されており、前記端末は更に、乱数である鍵データを生成する乱数データ発生手段と、デジタル著作物であるコンテンツデータを格納しているコンテンツ格納手段と、前記データ記録媒体から暗号化鍵特定情報を読み出し、前記復号鍵群記憶手段に記憶されている復号鍵群に呼応する暗号化鍵群のうち当該暗号化鍵特定情報で特定される暗号化鍵を選定する暗号化鍵選定手段と、前記暗号化鍵選定手段により選定された全ての暗号化鍵を逐次用いて前記乱数データ発生手段により生成された鍵データを暗号化することにより暗号化鍵データ群を生成して、当該暗号化鍵データ群を前記データ記録媒体に記録する鍵データ暗号化手段と、前記乱数データ発生手段により生成された鍵データを鍵として用いて前記コンテンツ格納部に格納されているコンテンツデータを暗号化することにより暗号化コンテンツデータを生成し、当該暗号化コンテンツデータを前記データ記録媒体に記録するコンテンツ暗号化手段とを備え、前記暗号化データ取得手段は、前記データ記録媒体に記録されている暗号化鍵データ及び暗号化コンテンツデータを取得し、前記復号手段は、前記暗号化データ取得手段により取得された前記暗号化鍵データを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号することにより鍵データを生成するものであり、前記端末は更に、前記暗号化データ取得手段により取得された前記暗号化コンテンツデータを、前記復号手段により生成された鍵データを用いて復号するコンテンツ復号手段を備えることを特徴とする請求項23記載の復号端末システム。

【請求項25】 前記暗号化されたデータは外部の送信装置から送信されるものであり、

前記暗号化データ取得手段は、前記暗号化されたデータを受信することにより取得することを特徴とする請求項22記載の復号端末システム。

【請求項26】 3台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定する暗号化鍵特定装置であって、

(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、

更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの1つの端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

2つ以上の端末集合を決定し、

(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵群対応付け手段と、

10

前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵設定手段と、

1つ以上の端末を無効化端末として特定する無効化端末特定手段と、

前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、

20

選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、

選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを備えることを特徴とする暗号化鍵特定装置。

【請求項27】 前記復号鍵設定手段は更に、前記複数の端末集合を完全に包含する端末集合が存在するよう

20

に、かつ、同じ1つ以上の端末集合を各々包含する複数の端末集合であって、当該複数の端末集合におけるいずれの1つの端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するよう、端末集合の前記決定を行うことを特徴とする請求項26記載の暗号化鍵特定装置。

【請求項28】 前記復号鍵設定手段は更に、各端末集合が3台以上の端末を要素に含むように、かつ、3つ以上の端末集合を包含する端末集合が存在するよう、端末集合の前記決定を行うことを特徴とする請求項27記載の暗号化鍵特定装置。

30

【請求項29】 前記復号鍵設定手段は、

各端末を各々別個の最下位層のノードに対応させた複数階層のN分木（Nは3以上の自然数）の木構造を想定した場合における最下位層を除く各ノードについて、当該ノード（親ノード）から辿り着く1段下位層のN個のノードのうち、2以上を組合せてなりN個全部の組合せを含む複数の組合せパターンを決定し、決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶しており、更に最下位層の各ノードに対応付けて別個の復号鍵を記憶しており、

前記復号鍵群対応付け手段は、

前記各端末について、当該端末に対応する最下位層のノードから最上位層のノードまでの経路上に位置する最下位層でない各ノードについて、当該ノードに対応付けて前記復号鍵設定手段により記憶されている復号鍵のうち、当該ノードの1段下位層で当該経路上に位置するノードを含む組合せに係る全ての前記組合せパターンに対応する復号鍵と、当該端末に対応付けて前記復号鍵設定

50

手段により記憶されている復号鍵とを、当該端末に対応付け、

前記各端末集合は、前記各組合せパターンと一対一に対応し、対応する組合せパターンにおいて組み合わされた全ノードから辿り着く最下位層のノードに対応する全ての端末を要素とする集合に相当し、前記暗号化鍵特定手段は、前記木構造を想定した場合において、いずれかの無効化端末に対応する最下位層のノードに辿り着く全てのノードを無効ノードと定め、まず最上位層ノードを処理対象ノードとしておき、未処理の処理対象ノードが存在しなくなるまで暗号化鍵特定処理を繰り返し行い、

前記暗号化鍵特定処理は、未処理の1つの処理対象ノードについて、

(a) 当該処理対象ノードの1段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在する場合には、当該組合せパターンに対応して前記復号鍵設定手段により記憶されている復号鍵に呼応する暗号化鍵を特定し、

(b) 当該処理対象ノードの1段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在しない場合には、当該1段下位層が最下位層であれば当該1段下位層における無効ノード以外の全てのノードに対応して前記復号鍵設定手段により記憶されている復号鍵に呼応する暗号化鍵を特定し、当該1段下位層が最下位層でなければ当該1段下位層における無効ノード以外の全てのノードを新たに処理対象ノードとし、

(c) 当該処理対象ノードの1段下位層において無効ノードが存在すれば、当該1段階層が最下位層でない限り全ての無効ノードを新たに処理対象ノードとする処理であることを特徴とする請求項28記載の暗号化鍵特定装置。

【請求項30】 前記復号鍵設定手段による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く1段下位層のN個のノードのうち、2以上を組合せてなる全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該復号鍵設定手段は、その各ノード（親ノード）について決定した全ての組合せパターンを、当該ノード（親ノード）から辿り着く前記N個のノードそれぞれを組合せ対象とするか否かを示す値を所定のノード順序に従って連結させてなる無効化パターン情報をとして当該ノード（親ノード）と対応付けて記憶するとともに、無効化パターン情報を毎に別個の復号鍵を定めて、その定めた各復号鍵を当該ノード（親ノード）及び当該無効化パターン情報を対応付けて記憶し、

前記暗号化鍵特定手段は、前記木構造を想定した場合において、いずれかの無効化端末に対応する最下位層のノードに辿り着く全てのノードを無効ノードと定め、最下位層を除く各ノードについて、当該ノードから辿り着く1段下位層のN個のノードそれぞれが無効ノードであるか否かを示す無効化情報を特定した後に、前記暗号化鍵特定処理を行い、

前記暗号化鍵特定処理は、未処理の1つの処理対象ノードについて、

(a) 当該処理対象ノードについて特定された無効化情報と整合する無効化パターン情報が存在する場合には、当該無効化パターン情報に対応して前記復号鍵設定手段により記憶されている復号鍵に呼応する暗号化鍵を特定し、

(b) 当該処理対象ノードについて特定された無効化情報と整合する無効化パターン情報が存在しない場合には、当該1段下位層が最下位層であれば当該1段下位層における無効ノード以外の全てのノードに対応して前記復号鍵設定手段により記憶されている復号鍵に呼応する暗号化鍵を特定し、当該1段下位層が最下位層でなければ当該1段下位層における無効ノード以外の全てのノードを新たに処理対象ノードとし、

(c) 当該処理対象ノードの1段下位層において無効ノードが存在すれば、当該1段階層が最下位層でない限り全ての無効ノードを新たに処理対象ノードとする処理であることを特徴とする請求項29記載の暗号化鍵特定装置。

【請求項31】 前記復号鍵設定手段による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く1段下位層のN個のノードのうち、N個全部の組合せ及び（N-1）個の全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該復号鍵設定手段は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることを特徴とする請求項29記載の暗号化鍵特定装置。

【請求項32】 3台以上の各端末への配給用データを暗号化する暗号化装置であって、

(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するよう、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの1つの端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するよう、

2つ以上の端末集合を決定し、

(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、

前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全

ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付け手段と、

1つ以上の端末を無効化端末として特定する無効化端末特定手段と、

前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、

選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段と、

前記暗号化鍵特定手段により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成する暗号化手段と、

前記暗号化手段により生成された暗号化配給用データ群を外部に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項33】 前記出力手段は、前記暗号化鍵特定手段により特定された各暗号化鍵を識別するための鍵特定情報を前記暗号化配給用データ群とともに外部に出力することを特徴とする請求項32記載の暗号化装置。

【請求項34】 前記暗号化装置は更に、
デジタル著作物であるコンテンツデータを記憶している
コンテンツ記憶手段と、
乱数である前記配給用データを生成する乱数データ発生
手段と、

前記乱数データ発生手段により生成された配給用データを鍵として用いて前記コンテンツデータを暗号化して、暗号化コンテンツデータを生成するコンテンツ暗号化手段とを備え、

前記出力手段は、前記コンテンツ暗号化手段により生成された暗号化コンテンツデータを前記暗号化配給用データ群とともに外部に出力することを特徴とする請求項32記載の暗号化装置。

【請求項35】 前記出力手段による前記出力は、前記暗号化配給用データ群をデータ記録媒体に記録することである。ことを特徴とする請求項32記載の暗号化装置。

【請求項36】 前記出力手段による前記出力は、前記暗号化配給用データ群を前記各端末に送信することであることを特徴とする請求項32記載の暗号化装置。

【請求項37】 3台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定するための暗号化鍵特定方法であって、

前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、

更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの1つの端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

10 前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、

1つ以上の端末を無効化端末として特定する無効化端末特定ステップと、

前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、

20 選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、

結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とする暗号化鍵特定方法。

【請求項38】 3台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定するための特定処理をコンピュータに実行させるためのコンピュータプログラムであって、
前記特定処理は、

前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、

更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの1つの端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

40 2つ以上の端末集合を決定する端末集合決定ステップと、

端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、

前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、

1つ以上の端末を無効化端末として特定する無効化端末

特定ステップと、

前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、

選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、

結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とするコンピュータプログラム。

【請求項39】 3台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定するための特定処理をコンピュータに実行させるためのコンピュータプログラムを記録した記録媒体であって、

前記特定処理は、

前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、

更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの1つの端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

2つ以上の端末集合を決定する端末集合決定ステップと、

端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、

前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、

1つ以上の端末を無効化端末として特定する無効化端末特定ステップと、

前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、

選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、

結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とする記録媒体。

【請求項40】 3台以上の各端末への配給用データが、特定処理により特定された複数の暗号化鍵それぞれを用いて暗号化されてなる複数の暗号化配給用データ

を、記録したコンピュータ読み取り可能な記録媒体であって、

前記特定処理は、

前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、

更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの1つの端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

2つ以上の端末集合を決定する端末集合決定ステップと、

端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、

前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、

1つ以上の端末を無効化端末として特定する無効化端末特定ステップと、

前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、

選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、

結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とする記録媒体。

【請求項41】 暗号化されたデータを取得して復号するための復号端末であって、

所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、

暗号化されたデータを取得する暗号化データ取得手段と、

前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段と、

前記所定鍵割当方法は、

(a) 本端末を含む3台以上の端末を想定した場合において本端末が、2つ以上の端末を要素に含む集合である複数の端末集合に属するように、

更に、本端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの1つの端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末

50

集合が存在するように、

2つ以上の端末集合を決定し、

(b) 本端末に対応して及び決定した端末集合毎に対応して各々別個の復号鍵を定め、

(c) 本端末に対して、本端末に対応して定めた復号鍵、及び本端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする復号端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データを複数の端末に暗号化して配給するデータ保護システムに関し、特に、データの暗号化及び復号に用いる鍵を決定する技術に関する。

【0002】

【従来の技術】近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からなるデジタルコンテンツを生成して光ディスク等の大容量記録媒体に格納して配布するシステムが現れている。配布された光ディスク等に記録されているデジタルコンテンツは、コンピュータや再生装置等の端末において読み出されて、再生、コピー等の対象となる。

【0003】かかるシステムにおいては一般的に、デジタルコンテンツに係るいわゆる著作権を保護するため、つまりデジタルコンテンツの不正コピー等といった不正利用を防止するために、暗号化技術が用いられる。即ち、かかるシステムは、デジタルコンテンツをある暗号化鍵を用いて暗号化して光ディスク等に記録して配布する。これに対し、その暗号化鍵に呼応する復号鍵を保持する端末のみが、光ディスク等から読み出したデータをその復号鍵を用いて復号して元のデジタルコンテンツを取得し、デジタルコンテンツの再生等を行うことができる。

【0004】なお、デジタルコンテンツを暗号化して記録媒体に記録する方法としては、端末が保持している復号鍵に呼応する暗号化鍵でデジタルコンテンツそのものを暗号化して記録する方法や、デジタルコンテンツをある鍵で暗号化して記録した上で、その鍵に呼応する復号用の鍵を端末が保持している復号鍵に呼応する暗号化鍵で暗号化して記録する方法等がある。

【0005】かかるシステムの一例として、例えば、「National Technical Report 第43巻第3号118頁～122頁」(松下電器産業株式会社 技術総務センター 平成9年6月18日発行)には、DVD著作権保護システムが開示されている。このDVD著作権保護システムにおいて配布されたDVDに記録されているデジタルコンテンツを再生するためのDVD再生端末は、その再生端末の製造メーカー毎に定められたマスタ鍵を予め保持しており、マスタ鍵を復号過程において用い、最終的にDVDに記録されたデジタル

コンテンツを復号し再生する機能を有する。なお、DVDには各メーカーのマスタ鍵で暗号化された、デジタルコンテンツの復号用に必要となる鍵群が記録されている。

【0006】

【発明が解決しようとする課題】ところで、通常、端末に保持されている復号鍵は秘密に保たれているが、端末の解析その他の方法で不正者が復号鍵を認識し暴露する可能性がある。ある端末に保持されている復号鍵が一旦暴露されてしまうと、不正者はこの復号鍵を用いてデジタルコンテンツの復号を行う端末やソフトウェア等を作成し、不正コピー等を行うおそれがあるので、結果的に、著作権保護のためには、暴露された復号鍵に呼応する暗号化鍵によりデジタルコンテンツを暗号化して光ディスク等に記録して配布することができなくなる。

【0007】例えば、上述のDVD著作権保護システムに係るDVD再生端末について考えると、1つのDVD再生端末が不正に解析される等によって一旦マスタ鍵が暴露された場合には、それ以後そのマスタ鍵により暗号化したデジタルコンテンツの配布ができなくなる。この結果、その暴露以後にはDVDの生成者等は、暴露されたのと別のマスタ鍵を用いた暗号化を施してデジタルコンテンツをDVDに記録して配布せざるを得なくなるが、不正者に解析等されたDVD再生端末と同一メーカーで製造された多数のDVD再生端末は、いずれも同じマスタ鍵を保持していることから、その暴露以後に新たに生成して配布したDVDに記録されているデジタルコンテンツの復号及び再生を行えなくなるという問題が生じる。即ち、1つのDVD再生端末が不正者に解析等されると、多数のDVD再生端末が将来において新たに生成されたDVDを利用できなくなってしまう。

【0008】この問題を解決するために、DVD再生端末毎に、別個の復号鍵を保持させておき、デジタルコンテンツ又はデジタルコンテンツの復号用に必要な鍵を、各DVD再生端末の保持する復号鍵に呼応する各暗号化鍵を用いて暗号化して得られる全ての暗号化データをDVDに記録する方法が考えられる。この方法によれば、一部のDVD再生端末が不正者に解析等され一部の復号鍵が暴露されても、それ以後においては、DVD再生端末群に保持されている暴露されていない各復号鍵に呼応する各暗号化鍵を用いたデジタルコンテンツ等の暗号化により得られる全ての暗号化データをDVDに記録して配布することができるため、暴露された復号鍵を保持するDVD再生端末以外の全てのDVD再生端末が、将来において新たに生成されたDVDを利用することができるようになる。

【0009】しかしこの方法も、DVDの配布対象として想定するDVD再生端末の数が膨大である場合には、DVDに記録すべき暗号化データが膨大になるという欠点を有する。そこで、本発明はかかる問題に鑑みてなされたものであり、デジタルコンテンツ、暗号化したデジ

タルコンテンツの復号に必要な鍵等のデータを暗号化して同一データを多数の端末に配給するデータ保護システムであって、配給対象の暗号化データの量の増大化をある程度抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合に、その特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるようにする暗号化技術を用いたデータ保護システムを提供すること、及びかかるデータ保護システムの構築に有用な技術を提供することを目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するため、本発明に係るデータ保護システムは、3台以上の端末、暗号化装置及び暗号化鍵特定装置を備え、各端末への配給用データを暗号化装置により暗号化して保護するデータ保護システムであって、前記各端末は、所定鍵割当方法により個別に割当てられた復号鍵群を記憶しており、前記暗号化装置から出力された暗号化配給用データ群を取得して、暗号化配給用データを、記憶している復号鍵を用いて復号するものであり、前記所定鍵割当方法は、(a)前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定し、(b)端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c)前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であり、前記暗号化鍵特定装置は、暗号化鍵を特定する装置であり、かつ、1つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記所定鍵割当方法により端末に割当てられた全ての復号鍵のうち無効化端末に割当てられた復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が割り当てられていない最も多くの端末に、割当てられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が割り当てられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを有する装置であり、前記暗号化装置は、前記暗号化鍵特定装置により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成して出力する暗号化手段を有することを特徴とする。

【0011】ここで、配給用データは、記録媒体に記録されて配布され、或いは有線又は無線の通信路を通じて配信され、最終的に各端末に到達することが想定される

データである。端末1、端末2、端末3を想定すれば、上述の所定鍵割当方法により決定される端末集合には、端末1及び端末2の組Aや、端末1及び端末3の組Bや、端末2及び端末3の組Cがあり、所定鍵割当方法による割り当て結果を受けて端末1が記憶保持する復号鍵は端末1固有の復号鍵と、組Aに対応する復号鍵Aと、組Bに対応する復号鍵Bとであり、端末2が記憶保持する復号鍵は端末2固有の復号鍵と、組Aに対応する復号鍵Aと、組Cに対応する復号鍵Cとであり、端末3が記憶保持する復号鍵は端末3固有の復号鍵と、組Bに対応する復号鍵Bと、組Cに対応する復号鍵Cである。この例において、端末2が不正に解析等されて端末2が記憶保持する全ての復号鍵が暴露されてしまった場合には端末2を無効化端末、つまり無効化にすべき端末として特定し、前記暗号化鍵特定手段による暗号化鍵の特定を行うと復号鍵Bに呼応する暗号化鍵が特定されることになる。

【0012】従って、復号鍵Bに呼応する暗号化鍵を用いてデータを暗号化して各端末に配給すれば、端末2では正しくそのデータを復号することができず、端末1及び端末3では正しくそのデータを復号することができる。同様の目的を、端末1固有の復号鍵に呼応する暗号化鍵と端末3固有の復号鍵に呼応する暗号化鍵とをそれぞれ用いてデータを暗号化して各端末に配給することもできるが、この方法と比べて前述の復号鍵Bに呼応する暗号化鍵を用いる方法は、暗号化に用いる暗号化鍵の数が少なく、その分だけ配給される暗号化データのデータ量が少なくなるという効果を有する。

【0013】即ち、本発明によれば、暗号化したデジタルコンテンツの復号に必要な鍵等のデータを暗号化して同一データを複数の端末に配給するデータ保護システムにおいて、配給対象の暗号化データの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合に、その特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるようにすることが可能となる。

【0014】また、本発明に係る復号鍵決定装置は、暗号化されたデータを取得して復号するための3台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定装置であって、(a)前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定し、(b)端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、前記各端末に対して、

前記復号鍵設定手段により当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当手段とを備えることを特徴とする。

【0015】また、本発明に係る復号鍵決定方法は、暗号化されたデータを取得して復号するための3台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定方法であって、前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定する端末集合決定ステップと、端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当ステップとを含むことを特徴とする。

【0016】また、本発明に係る復号端末システムは、暗号化されたデータを取得して復号するための3台以上の端末から構成される復号端末システムであって、前記各端末は、所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、暗号化されたデータを取得する暗号化データ取得手段と、前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段とを備え、前記所定鍵割当方法は、(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c) 前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする。

【0017】また、本発明に係る復号端末は、暗号化されたデータを取得して復号するための復号端末であって、所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、暗号化されたデータを取得する暗号化データ取得手段と、前記暗号化データ

タ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段と、前記所定鍵割当方法は、(a) 本端末を含む3台以上の端末を想定した場合において本端末が、2つ以上の端末を要素に含む集合である複数の端末集合に属するよう、更に、本端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定し、(b) 本端末に対応して及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c) 本端末に対して、本端末に対応して定めた復号鍵、及び本端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする。

【0018】これらにより、例えば、各端末へ記録媒体に暗号化された結果のデータを記録して記録媒体を配布する場合において、その記録媒体に記録されるデータの量の増大化を抑制した上で、特定の端末の解析等により20 その端末が保持していた復号鍵が不正者によって暴露された場合にその特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるように、その暗号化を実施することが可能になる。

【0019】また、本発明に係る暗号化鍵特定装置は、3台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定する暗号化鍵特定装置であって、(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵群対応付け手段と、前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵設定手段と、1つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したとき、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを備えることとを特徴とする。

【0020】また、本発明に係る暗号化装置は、3台以上の各端末への配給用データを暗号化する暗号化装置であって、(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するよう、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するよう、2つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付け手段と、1つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられる復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段と、前記暗号化鍵特定手段により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成する暗号化手段と、前記暗号化手段により生成された暗号化配給用データ群を外部に出力する出力手段とを備えることを特徴とする。

【0021】また、本発明に係る暗号化鍵特定方法は、3台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定するための暗号化鍵特定方法であって、前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するよう、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するよう、2つ以上の端末集合を決定する端末集合決定ステップと、端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、1つ以上の端末を無効化端末として特定する無効化端末特定ステップと、前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効

化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とする。

【0022】これらにより、例えば、各端末へ記録媒体10に暗号化された結果のデータを記録して記録媒体を配布する場合において、暗号化に用いる暗号化鍵の数を比較的少なく抑えることができるので、その記録媒体に記録されるデータの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合にその特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるように、その暗号化を実施することが可能になる。

【0023】

【発明の実施の形態】<実施の形態1>以下、本発明の20実施の形態1に係るデータ保護システムについて図を用いて説明する。

<全体構成>図1は、本発明の実施の形態1に係るデータ保護システム100の概略構成図である。

【0024】データ保護システム100は、同図に示すように、暗号化装置101、複数の復号装置(端末)103a～103n及び鍵設定システム104を備え、映像、音声等を示すデジタルデータからなるコンテンツを暗号化してDVD-ROM等である光ディスク102に記録して、複数の端末に配布するためのシステムである。

【0025】ここで、鍵設定システム104は、暗号化装置101に設定するための暗号化鍵、及び復号装置103a～103nに個別に設定するための復号鍵を決定するシステムである。暗号化装置101は、鍵設定システム104により特定された暗号化鍵を保持しており、コンテンツを暗号化して、光ディスク102に記録する装置である。なお、光ディスク102については、完全に同一な記録内容を有する物が多数複製されることが想定される。

【0026】また、復号装置103a～103nは、例えば10億台といった多数の端末であり、各復号装置は、それぞれ個別に鍵設定システム104により決定された復号鍵を保持しており、光ディスク102から暗号化されたコンテンツ(以下、「暗号化コンテンツ」という。)を読み出して復号し、復号により得られるコンテンツを再生する装置である。

【0027】なお、データ保護システム100をコンテンツに係る著作権の保護を行うために用いる場合には、鍵設定システム104及び暗号化装置101は著作権保護の管理を行う機関に運用され、復号装置は一般ユーザ

に利用されることになると想定される。また、鍵設定システム104は、基本的に、各復号装置用の復号鍵を決定するために1度利用され、最初に用いられる暗号化鍵を特定するために1度利用され、更に、特定の復号装置が不正に解析される等によりその復号装置に保持されている復号鍵が暴露されたことが判明した都度、その特定の復号装置では光ディスクに記録された暗号化コンテンツの復号を行えないようにすることを目的として、暗号化装置101で新たにコンテンツを光ディスクに記録する際に用いられるべき新たな暗号化鍵を特定するために利用される。

【0028】以下、暗号化装置101、復号装置103a～103n及び鍵設定システム104について、より詳細に説明する。

＜暗号化装置の構成＞図2は、暗号化装置101及び復号装置103aの機能構成図である。同図に示すように暗号化装置101は、コンテンツ記憶部201、乱数発生部202、暗号化鍵群格納部203、鍵暗号化部204、コンテンツ暗号化部205及び出力部206を有する。

【0029】ここで、コンテンツ記憶部201は、映像、音声等を示すデジタルデータからなるコンテンツを記憶しているハードディスク等の記憶装置である。乱数発生部202は、コンテンツの暗号化に用いられる鍵（以下、「コンテンツ鍵」という。）となる乱数を発生する機能を有する。なお、コンテンツ鍵は、乱数からなる例えば64ビットのデータである。

【0030】暗号化鍵群格納部203は、鍵設定システム104により特定された1又は複数の暗号化鍵を格納し、また、格納している暗号化鍵に呼応する復号鍵を復号装置側が特定するために用いられる鍵特定情報を格納するメモリ等の記憶装置である。なお、鍵設定システム104の運用により新たに暗号化鍵の特定が行われた場合には、暗号化鍵群格納部203にその特定前に保持されていた暗号化鍵は削除され、新たに特定された暗号化鍵のみが暗号化鍵群格納部203に格納される。この新たな暗号化鍵及びその暗号化鍵に対応する鍵特定情報の格納は、例えばオペレータにより入力されることによってなされることとしてもよいし、鍵設定システム104からの受信によりなされることとしてもよい。

【0031】鍵暗号化部204は、乱数発生部202から取得したコンテンツ鍵を、暗号化鍵群格納部203に格納された各暗号化鍵を用いて暗号化し、その結果である暗号化されたコンテンツ鍵（以下、「暗号化コンテンツ鍵」という。）それぞれを出力部206に伝える機能を有する。コンテンツ暗号化部205は、コンテンツ記憶部201に記憶されているコンテンツを、乱数発生部202から取得したコンテンツ鍵を用いて暗号化し、その結果である暗号化コンテンツを出力部206に伝える機能を有する。

【0032】また、出力部206は、データを光ディスクに記録可能なハードウェアを含み、暗号化鍵群格納部203から鍵特定情報を取得し、その鍵特定情報と、コンテンツ暗号化部205から伝えられた暗号化コンテンツと、鍵暗号化部204から伝えられた暗号化コンテンツ鍵とを、光ディスク102へ記録する機能を有する。

【0033】この暗号化装置101の記録により、光ディスク102には、暗号化コンテンツと、1又は複数の暗号化コンテンツ鍵と、鍵特定情報とが記録されることになる。なお、光ディスク102に記録される暗号化コンテンツ鍵の数は、鍵設定システム104により特定されて暗号化鍵群格納部203に格納されている暗号化鍵の数と一致する。

【0034】このような暗号化装置101は、ハードウェアとしてはCPU、メモリ等を備えており、上述した乱数発生部202、鍵暗号化部204、コンテンツ暗号化部205及び出力部206の機能の全部又は一部はメモリに格納された制御用プログラムがCPUにより実行されることにより実現されるものである。

20 <復号装置の構成>復号装置103aは、光ディスク再生用の端末であり、図2に示すように取得部211、復号鍵群格納部212、復号鍵選定部213、鍵復号部214、コンテンツ復号部215及び再生部216を有する。

【0035】ここで、取得部211は、光ディスクからデータを読み出し可能なハードウェアを含み、光ディスク102から暗号化コンテンツを読み出してコンテンツ復号部215に伝え、光ディスク102から暗号化コンテンツ鍵を読み出して鍵復号部214に伝え、光ディスク102から鍵特定情報を読み出して復号鍵選定部213に伝える機能を有する。

30 【0036】復号鍵群格納部212は、鍵設定システム104により復号装置103aに対して決定された複数の復号鍵等を格納する不揮発性メモリ等の記憶装置である。復号鍵の格納は、例えば復号装置の製造工程においてなされる。復号鍵選定部213は、取得部211から伝えられる鍵特定情報に基づいて、復号鍵群格納部212に格納されている復号鍵群のうちどの復号鍵を用いることができるかを判定し、用いることができる1つの復号鍵を選定する機能を有する。

【0037】鍵復号部214は、復号鍵選定部213により選定された復号鍵を用いることにより復号可能な暗号化コンテンツ鍵を、取得部211を通じて取得し、取得した暗号化コンテンツ鍵をその復号鍵を用いて復号することによりコンテンツ鍵を生成する。コンテンツ復号部215は、取得部211から伝えられる暗号化コンテンツを、鍵復号部214により生成されたコンテンツ鍵を用いて復号することによりコンテンツを生成して再生部216に伝える機能を有する。

50 【0038】また、再生部216は、コンテンツ復号部

215から伝えられたコンテンツを再生する機能を有する。なお、データ保護システム100の扱うコンテンツが、例えばMPEG (Moving Picture Expert Group) 等で規定された圧縮方式に従った動画データであることとしたならば、再生部216は、例えば、いわゆるMPEGデコーダ等であって、コンテンツを伸長して映像信号を出力する機能を含む必要がある。

【0039】このような復号装置103aは、ハードウェアとしてはCPU、メモリ等を備えており、上述した取得部211、復号鍵選定部213、鍵復号部214、コンテンツ復号部215及び再生部216の機能の全部又は一部はメモリに格納された制御用プログラムがCPUにより実行されることにより実現されるものである。

【0040】なお、復号装置103a以外の複数の復号装置103b～103nも、復号装置103aと同様の構成を備える。但し、復号鍵群格納部212に格納されている内容の全部又は一部は復号装置毎に異なる。

＜鍵設定システムの構成＞図3は、鍵設定システム104の機能構成図である。

【0041】同図に示すように鍵設定システム104は、鍵情報格納部301、鍵情報生成部302、無効化端末特定部303、鍵情報更新部304、復号鍵決定部305及び暗号化鍵特定部306を有する。ここで、鍵情報格納部301は、後述する鍵情報を格納するためのハードディスク等の記憶装置である。

【0042】鍵情報生成部302は、データ保護システム100を構成する復号装置それぞれを階層的な4分木の木構造の最下位層のノードに対応させるように木構造を決定し、木構造における各ノードについて1又は複数の鍵を割り当て、各ノードについて割り当てられた鍵等を示す鍵情報を生成する。なお、鍵情報は、暗号化鍵及び復号鍵を特定するために用いられるための情報であり、各ノードについて割り当てられた各鍵を暗号化鍵として用いることができるか否かの判断基準となる無効化情報を含む。この鍵情報及び4分木の木構造については後に詳しく説明する。

【0043】無効化端末特定部303は、キーボード、ポインティングデバイス等の入力装置を介してオペレータから、保持している復号鍵が暴露された復号装置の指定を受け付け、その指定された復号装置を無効化すべき端末（以下、「無効化端末」という。）として特定する機能を有する。無効化端末は、コンテンツの暗号化において、その端末では暗号化コンテンツの復号が正しく行えないように、暗号化を行う必要がある復号装置を示す。

【0044】鍵情報更新部304は、無効化端末特定部303により特定された無効化端末に基づいて、鍵情報格納部301に格納されている鍵情報中の無効化情報を更新する機能を有する。復号鍵決定部305は、鍵情報

格納部301に格納されている鍵情報に基づいて復号装置それぞれについて設定すべき複数の復号鍵を決定する機能を有する。なお、各復号装置について決定された復号鍵は、その復号鍵について、鍵情報により対応付けられていたノードを示す情報とともにその復号装置の復号鍵群格納部に、例えば復号装置の製造工程において、格納される。従って、鍵設定システム104は、例えば、決定した復号鍵、及び復号鍵とノードとの対応を示す情報を例えば復号装置の製造用の製造システムに送信する。

【0045】また、暗号化鍵特定部306は、鍵情報格納部301に格納されている鍵情報に基づいて暗号化装置に設定すべき1又は複数の暗号化鍵を特定する機能を有し、特定した暗号化鍵とノードとの対応を示すことにより復号時にどの復号鍵を用いるとよいかの判断基準となる鍵特定情報をその特定した暗号化鍵とともにに出力する。

【0046】この出力は、例えば、暗号化装置101への送信や、可搬性のある記録媒体への記録である。なお、暗号化鍵特定部306が暗号化鍵を可搬性のある記録媒体へ記録する場合には、運用上、オペレータによりその記録媒体の内容が暗号化装置101の暗号化鍵群格納部203にコピーされる必要がある。

＜鍵情報＞以下、鍵情報生成部302により生成され、鍵情報格納部301に格納される鍵情報について説明する。

【0047】まず、4分木の木構造について説明する。図4は、4分木の木構造を示す図である。この木構造は、最下位層のノード群406を構成する各ノード（以下、「リーフ」ともいう。）と復号装置（端末）とが1対1で対応するように構築され、1つのノードからは4つのノードへの分岐を持つ木構造である。なお、ここでは、この1つのノードからn個のノードへの分岐を持つ構造をn分木と称しており、4個のノードへの分岐を持つ構造であれば4分木と称する。また、その4つのノードへの分岐を持つ1つのノードをその4つのノードに対して親ノードと称し、親ノードに対してその4つのノードを子ノードと称し、最上位層のノード405をルートと称することとする。

【0048】データ保護システム100における復号装置の数が、4の階乗数でない場合には、最下位層のノード数は、復号装置の数より大きい4の階乗数のうち最小の数となるが、ここでは、説明の簡単化のために、復号装置の数は最下位層のノード数と一致することとする。鍵情報生成部302は、図4に示す木構造の最上位層401をレベル0、1つ下の層402をレベル1と、順次1つ下の層をレベルを1つ増加して、最下位層の1つ上の層403をレベルD-1、最下位層404をレベルDと定め、各レベルにおける各ノードは、各レベルにおける相対番号を1から順にそれぞれ定める。従って、レベ

ルDにおける相対番号1のノードは復号装置103aに対応し、レベルDにおける相対番号2のノードは復号装置103bに対応し、レベルDにおける相対番号4のD乗のノードは最後の復号装置103nに対応する。

【0049】図5は、復号装置数が64台である場合における4分木の木構造の例を示す図である。同図に示す例では、リーフが64個存在するように4分木の木構造が構築されるため、最下位層はレベル3となる。次に、各ノードに対応して定める無効化情報について説明する。

【0050】あるノードについての無効化情報は、そのノードを親ノードとした場合の4つの子ノードについて、そのノードが無効ノードであるか否かを示すフラグを、相対番号の小さいノードについてのフラグから順に結合した情報である。その、フラグは無効ノードであれば1、無効ノードでなければ0の値をとる。従って、例えば4つの子ノードが無効ノードでなければ親ノードの無効化情報は"0000"となり、4つの子ノードが無効ノードであれば親ノードの無効化情報は"1111"となる。

【0051】但し、リーフについては無効化情報は、リーフに対応する復号装置が無効化端末であれば"1111"で無効化端末でなければ"0000"となることとする。なお、無効ノードとは、無効化端末に対応するリーフであるか、又は無効化端末に対応するリーフから上層に向けて辿り着くノードをいう。従って、無効ノードは、対応する無効化情報が"0000"以外の値をとるノードであるとも言える。

【0052】ここで、特定のノードから「辿り着く」ノードとは、親ノードと子ノードとの関係にある各ノード間にはチェーンが張られていると想定した場合において、その特定のノードから上層方向及び下層方向のいずれか一方向に向けての1又は複数のチェーンにより、繋がっているノードをいう。従って、木構造において、上層のノードから終始下層方向に向けて1又は複数のチェーン上を通ることにより到達する下層のノードは、その上層のノードから辿り着くノードであり、逆にその上層のノードはその下層のノードから辿り着くノードである。例えば、いずれのリーフからもルートに辿りつき、ルートからもいずれのリーフに辿り着くが、あるリーフから他のリーフには辿り着くことはない。

【0053】復号装置の保持する復号鍵が暴露される前においては、無効化端末は存在しないため、全てのノードについての無効化情報は"0000"の値をとる。図6及び図7は、ルートの無効化情報の例を示す図である。図6の例は、ルートの子ノードは全て無効ノードでない場合におけるルートの無効化情報は"0000"となることを示している。

【0054】図7の例は、無効ノードを×印により示しており、ルートの子ノードのうち相対番号が1であるも

のだけが無効ノードである場合におけるルートの無効化情報は"1000"となることを示している。次に、各ノードについて割り当てられる鍵について説明する。鍵情報生成部302により、各ノードについて別個に、暗号化鍵と、その暗号化鍵に呼応する復号鍵の組が割り当てられる。なお、リーフについては復号装置毎に固有の1組の鍵が割り当てられ、リーフ以外のノードについては以下に示すように複数組の鍵が割り当てられることがある。

10 【0055】図8は、4分木の木構造のレベル0及びレベル1の階層のノードに対応して割り当てられる鍵を示す図である。同図中、0-1K0000、0-1K0001等は、暗号化鍵及びそれに呼応する復号鍵を、便宜上まとめて表現したものである。なお、データ保護システム100において暗号化鍵と復号鍵とは別個の値をとる方式又は同一の値をとる方式のいずれを採用するかを予め定めておくことができ、暗号化鍵と復号鍵とは別個の値をとる方式を採用する場合には、例えば0-1K0000で表される復号鍵と0-1K0000で表される暗号化鍵は別個の値のものとなり、データ保護システム100において暗号化鍵と復号鍵とは同一の値をとる方式を採用する場合には、例えば0-1K0000で表される暗号化鍵及び復号鍵は同一の値のものとなる。

20 【0056】以下、各ノードには復号鍵が割り当てられているという表現又は各ノードには暗号化鍵が割り当てられているという表現を用いるが、実際には復号鍵と暗号化鍵とが別個の値をとる方式を採用する場合においては復号鍵とそれに呼応する暗号化鍵が各ノードに割り当てられており、復号鍵と暗号化鍵とが同一の値をとる方式を採用する場合においては、復号鍵でもあり暗号化鍵でもある鍵が各ノードに割り当てられていることになる。これにより、鍵情報中に割り当てられた復号鍵等が設定されることになる。なお、暗号化鍵及び復号鍵は、例えば64ビットのデータである。

30 【0057】図8に示すように、リーフ以外のノードについては、11個の復号鍵が割り当てられている。ここでは、あるノードについての無効化情報のとり得る"0000"、"1000"等の値のうち、"1"の数がn分木の木構造である場合における(n-1)個未満となる値を無効化パターンと称する。従って、4分木における無効化パターンは、"1"の数が3未満となるところの"0000"、"0001"、"0010"、"0011"、"0100"、"0101"、"0110"、"1000"、"1001"、"1010"及び"1100"の11種類存在し、リーフ以外の各ノードには、全無効化パターン分の11個の復号鍵が割り当てられている。

40 【0058】ここでは、レベルAの相対番号Bのノードについての鍵であって、無効化パターンがXであるものを、「A-BKX」と表現している。従って「0-1K

「0000」は、レベル0の相対番号1のノードについての無効化パターンが“0000”に対応する復号鍵等であることを示している。図9は、鍵情報格納部301に格納される鍵情報の構成を示す図である。

【0059】同図に示すように鍵情報500は、各ノードについて、そのノードのノードID501と無効化パターン502と鍵503と無効化情報504とが対応付けられた情報である。ノードID501は、木構造におけるノードの所在位置を示すレベルと相対番号とを示すIDであり、例えばレベルAの相対番号BのノードのノードIDは「A-B」と表現される。

【0060】無効化パターン502は、上述のように無効化情報のとり得る値のうち“1”的数が3未満となる値である。鍵503は、対応するノードIDで示されるノードに割り当てられている復号鍵及び暗号化鍵である。無効化情報504は、対応するノードIDで示されるノードについての無効化情報であり、初期値は“00”である。

【0061】なお、鍵情報中、リーフに対応する無効化パターンはなく、リーフについての鍵503は1組の復号鍵及び暗号化鍵である。

〈鍵割当処理〉以下、鍵設定システム104における鍵情報生成部302により鍵情報格納部301に鍵情報が格納された後に、復号鍵決定部305が、全ての復号装置103a～103nそれぞれに設定すべき復号鍵を決定するために行う、即ち各復号装置に複数の復号鍵を割り当てるために行う鍵割当処理について説明する。

【0062】図10は、復号鍵決定部305により実行される鍵割当処理を示すフローチャートである。復号鍵決定部305は、まず復号装置(端末)のうち4分木の木構造におけるリーフの相対番号1が対応付けられた復号装置を割当対象端末とし(ステップS11)、割当対象端末に対応するリーフ即ち最下位層のノードに着目してそのノード(着目ノード)に割り当てられている1つの復号鍵を特定する(ステップS12)。なお、ノードへの着目とは、具体的には例えば、鍵情報中のそのノードについての情報の記憶領域内アドレスを内部処理用の変数等に格納すること等をいう。

【0063】続いて、復号鍵決定部305は、着目ノードが有効であること即ち無効ノードでないことを示すところの、着目ノードの一層上のノード(親ノード)について、鍵情報格納部301に格納されている鍵情報において定められている無効化パターンに対応する復号鍵を全て特定し、その親ノードを新たに着目ノードと定める(ステップS13)。

【0064】ステップS13に続いて、復号鍵決定部305は、現在の着目ノードはルートであるか判定し(ステップS14)、ルートでなければ、現在の着目ノードがルートとなるまでステップS13の処理を繰り返し行う。ステップS14において現在の着目ノードがルート

であれば、復号鍵決定部305は、割当対象端末に対してステップS12及びステップS13で特定した全ての鍵を設定すべき復号鍵として決定し(ステップS15)、割当対象端末は、最後の端末か否か、即ち、リーフのうち相対番号が最も大きいものに対応付けられている復号装置か否かを判定し(ステップS16)、最後の端末であれば鍵割当処理を終える。

【0065】また、ステップS16において割当対象端末が最後の端末でないと判定した場合には、復号鍵決定部305は、現在の割当対象端末の次ぎの端末、即ち現在の割当対象端末に対応するリーフよりも相対番号が1つ大きいリーフに対応付けられている復号装置を、新たに割当対象端末と定めて(ステップS17)、ステップS12の処理を行う。

【0066】このような鍵割当処理により、各復号装置に対して設定されるべき復号鍵群が決定され、これを受けて、各復号装置はそれぞれ決定された復号鍵群を保持するように構成される。図11は、64台しか復号装置がないと仮定した場合においてレベル3の相対番号1のリーフに対応する復号装置(端末1)に割り当てられるものと鍵割当処理によって決定される復号鍵群905を示す図である。

【0067】なお、同図中の3-1Kは、レベル3の相対番号1のリーフ904に唯一割り当てられている復号鍵を表したものである。64台しか復号装置がないと仮定した場合においては、図11に示すように、端末1には、レベル3の相対番号1のリーフ904に割り当てられている復号鍵3-1Kと、そのリーフの1層上の親ノードであるレベル2の相対番号1のノード903について割り当てられている復号鍵のうち、1番目の子ノードが無効ノードでないことを示す無効化パターンに対応する復号鍵、即ち“0000”、“0001”、“0010”、“0011”、“0100”、“0101”及び“0110”という7つの無効化パターンに対応する7つの復号鍵2-1K0000、2-1K0001、2-1K0010、2-1K0011、2-1K0100、2-1K0101及び2-1K0110と、そのさらに1層上の親ノードであるレベル1の相対番号1のノード902について割り当てられている復号鍵のうち、1番目の子ノードが無効ノードでないことを示す無効化パターンに対応する7つの復号鍵1-1K0000、1-1K0001、1-1K0010、1-1K0011、1-1K0100、1-1K0101及び1-1K0110と、そのさらに1層上の親ノードであるレベル0の相対番号1のノード即ちルート901について割り当てられている復号鍵のうち、1番目の子ノードが無効ノードでないことを示す無効化パターンに対応する7つの復号鍵0-1K0000、0-1K0001、0-1K0010、0-1K0011、0-1K0100、0-1K0101及び0-1K0110との合計22個の

復号鍵が割り当てられる。

【0068】従って、この場合には端末1の復号鍵群格納部212にはその割り当てられた22個の復号鍵が、例えは端末1の製造工程等において、格納されることになる。なお、リーフ以外の各ノードに対応する無効化パターンは、そのノードの子ノードが無効ノードであれば”1”を無効ノードでない有効ノードであれば”0”を、子ノードのレベル内相対番号の小さい順に連結した情報であり、無効化パターンに復号鍵を割り当てることは、無効化パターンにおいて有効ノードと示される全ての子ノードから辿り着くことのできる全てのリーフに対応する全端末を要素とする端末集合に対して復号鍵を割り当てることに相当する。従って、各端末には、その端末固有の復号鍵と、その端末を含む全ての端末集合に割り当てられている復号鍵とが割り当てられることになる。

【0069】<暗号化鍵の特定>鍵設定システム104の暗号化鍵特定部306は、無効化端末がない状態、即ちどの復号鍵も暴露されていない状態においては、ルートに割り当てられている暗号化鍵0-1K0000、つまり復号鍵0-1K0000に呼応する暗号化鍵を、暗号化装置101の暗号化鍵群格納部203に設定すべき暗号化鍵として特定する。

【0070】これに対し暗号化装置101は、この特定された暗号化鍵と、木構造におけるルートに割り当てられている復号鍵0-1K0000を特定する鍵特定情報を、鍵設定システム104から受信する等によって、暗号化鍵群格納部203に格納している。光ディスク102へコンテンツを記録する場合には、暗号化装置101は、乱数発生部202から生成されたコンテンツ鍵を、暗号化鍵群格納部203に格納している暗号化鍵を用いて鍵暗号化部204において暗号化し、その暗号化により得られる暗号化コンテンツ鍵を鍵特定情報と対応付けて、出力部102により光ディスク102に記録し、また、コンテンツ鍵を用いてコンテンツ記憶部201に記憶されているコンテンツをコンテンツ暗号化部205において暗号化し、その暗号化により得られる暗号化コンテンツを出力部102により光ディスク102に記録する。

【0071】以下、鍵設定システム104における鍵情報更新部304により実行される無効化情報更新処理について説明する。無効化端末特定部303により無効化端末が特定された場合に鍵情報更新部304は、鍵情報格納部301に格納されている鍵情報のうち、無効化端末に対応する4分木の木構造におけるリーフについての無効化情報を”1111”にして、そのリーフが無効ノードであることを示すようにした後に、鍵情報のうち各ノードに対応する無効化情報を更新する無効化情報更新処理を行う。

【0072】図12は、鍵情報更新部304により実行

される無効化情報更新処理を示すフローチャートである。まず、鍵情報更新部304は、4分木の木構造における最下位層の1層上の層に着目する（ステップS21）。つまり、最下位層がレベルDであれば、レベル（D-1）の層に着目する。

【0073】続いて鍵情報更新部304は、着目している層（着目層）の各ノードに相対番号の小さい順に順次着目し、その着目しているノード（着目ノード）の4つの子ノードについての無効ノードの組合せパターンに合致するように、着目ノードについての無効化情報を更新する（ステップS22）。例えば、着目ノードの4つの子ノードが相対番号の小さい順に、「無効ノード」、「無効ノードでない」、「無効ノードでない」、「無効ノードでない」ものであった場合には、着目ノードについての無効化情報は”1000”となる。

【0074】ステップS22の後に、鍵情報更新部304は、現在の着目層は最上位層即ちレベル0の層であるかを判定し（ステップS23）、最上位層でなければ、着目層の1つ上の層に着目し（ステップS24）、ステップS22の処理を行う。鍵情報更新部304は、ステップS23の判定において、現在の着目層が最上位層になるまで、ステップS22～S24を繰り返し、ステップS23の判定において現在の着目層が最上位層になれば、無効化情報更新処理を終える。

【0075】この結果として、4分木の木構造において無効化端末に対応するリーフから上層に向けて辿ると到達できる全てのノードについての無効化情報は”0000”以外の値をとることになる。次に鍵設定システム104の無効化端末特定部303により無効化端末が特定され、鍵情報更新部304により鍵情報中の無効化情報が更新された後に、暗号化鍵特定部306が、暗号化装置101の暗号化鍵群格納部203に設定すべき暗号化鍵群を特定するために行う鍵特定処理について説明する。

【0076】図13は、暗号化鍵特定部306により実行される鍵特定処理を示すフローチャートである。まず、暗号化鍵特定部306は、4分木の木構造における最上位層のノード、即ちルートに着目する（ステップS31）。続いて暗号化鍵特定部306は、着目しているノード（着目ノード）について、鍵情報格納部301に格納されている鍵情報を参照して、その着目ノードの無効化情報を合致する無効化パターンが存在するかを判定し（ステップS32）、もし無効化パターンが存在する場合にはその着目ノードについてのその無効化パターンに対応する暗号化鍵を、暗号化装置101に設定すべき暗号化鍵として特定し（ステップS33）、着目ノードの1層下の層が木構造における最下位層でないと判定した場合に限り（ステップS34）、着目ノードの子ノードのうち無効ノードが存在すればその全ての無効ノードを着目予定ノードと定める（ステップS35）。

【0077】ステップS32において、無効化情報に合致する無効化パターンが存在しないと判定した場合は、暗号化鍵特定部306は、着目ノードの子ノードの属する層は木構造における最下位層か否かを判定し（ステップS36）、着目ノードの子ノードの属する層が最下位層であれば着目ノードの子ノードのうち無効化端末に対応するリーフ以外のものに割り当てられている暗号化鍵を、暗号化装置101に設定すべき暗号化鍵として特定する（ステップS37）。

【0078】ステップS36において、着目ノードの子ノードの属する層が最下位層でないと判定した場合は、暗号化鍵特定部306は、着目ノードの全ての子ノードを着目予定ノードと定める（ステップS38）。ステップS35、S37、S38の後、或いはステップS34において着目ノードの1層下の層が最下位層であると判定した後に、暗号化鍵特定部306は、未だ着目していない着目予定ノードが存在するか否かを判定し（ステップS39）、未だ着目していない着目予定ノードが存在する場合には未着目の着目予定ノードのうちの1つのノードに新たに着目し（ステップS40）、ステップS32の判定処理に戻る。

【0079】また、ステップS39において、未だ着目していない着目予定ノードが存在しないと判定した場合には、暗号化鍵特定部306は、鍵特定処理を終える。この結果、ステップS33又はS37により特定された全ての暗号化鍵が、鍵特定情報とともに暗号化鍵特定部306から出力され、暗号化装置101の暗号化鍵群格納部203に格納されることになる。

【0080】図14は、64台しか復号装置がないと仮定した場合において、無効化端末がない状態での暗号化鍵等を示す図である。この場合において、暗号化装置101の暗号化鍵群格納部203に格納される暗号化鍵であって、コンテンツの光ディスク102への記録に際してコンテンツ鍵の暗号化に用いられることとなる暗号化鍵は、暗号化鍵0-1K0000、つまり0-1K000で表される復号鍵に呼応する1つの暗号化鍵となる。

【0081】図15は、64台しか復号装置がないと仮定した場合において、端末1が無効化端末である状態での暗号化鍵等を示す図である。端末1のみが無効化端末であると、上述した無効化情報更新処理の結果として、鍵情報格納部301に格納されている鍵情報については、レベル2の層の相対番号1番のノード1103の無効化情報が"1000"となり、レベル1の層の相対番号1番のノード1102の無効化情報が"1000"となり、レベル0の層のルート1101の無効化情報が"1000"となる。

【0082】このことを前提として、以下、図15の例に基づいて、上述した鍵特定処理（図13参照）の具体的処理内容を説明する。まず、暗号化鍵特定部306

は、最上位層のノード、即ちルート1101に着目する（ステップS31）。続いて暗号化鍵特定部306は、着目しているノード（着目ノード）について、鍵情報格納部301に格納されている鍵情報を参照して、そのノード1101の無効化情報である"1000"は、上述した11種類の無効化パターンの1つと合致するので（ステップS32）、その無効化パターンに対応する暗号化鍵0-1K1000を、暗号化装置101に設定すべき暗号化鍵として特定し（ステップS33）、着目ノードの1層下の層はレベル1の層であり最下位層ではないため（ステップS34）、着目ノードの子ノードのうちに存在する無効ノードであるノード1102を着目予定ノードと定める（ステップS35）。

【0083】ステップS35の後、暗号化鍵特定部306は、未だ着目していない着目予定ノードとしてノード1102が存在するので（ステップS39）、ノード1102を新たに着目ノードとして（ステップS40）、ステップS32の判定処理に戻る。続いて暗号化鍵特定部306は、着目ノードについて、鍵情報格納部301に格納されている鍵情報を参照して、そのノード1102の無効化情報である"1000"は、上述した11種類の無効化パターンの1つと合致するので（ステップS32）、その無効化パターンに対応する暗号化鍵1-1K1000を、暗号化装置101に設定すべき暗号化鍵として特定し（ステップS33）、着目ノードの1層下の層はレベル2の層であり最下位層ではないため（ステップS34）、着目ノードの子ノードのうちに存在する無効ノードであるノード1103を着目予定ノードと定める（ステップS35）。

【0084】ステップS35の後、暗号化鍵特定部306は、未だ着目していない着目予定ノードとしてノード1103が存在するので（ステップS39）、ノード1103を新たに着目ノードとして（ステップS40）、ステップS32の判定処理に戻る。続いて暗号化鍵特定部306は、着目ノードについて、鍵情報格納部301に格納されている鍵情報を参照して、そのノード1103の無効化情報である"1000"は、上述した11種類の無効化パターンの1つと合致するので（ステップS32）、その無効化パターンに対応する暗号化鍵2-1K1000を、暗号化装置101に設定すべき暗号化鍵として特定し（ステップS33）、着目ノードの1層下の層はレベル3の層であり最下位層であるため（ステップS34）、ステップS35をスキップし、未だ着目していない着目予定ノードはもう存在しないので（ステップS39）、鍵特定処理を終える。

【0085】この鍵特定処理の結果として、暗号化装置101の暗号化鍵群格納部203に格納される暗号化鍵群であって、コンテンツの光ディスク102への記録に際してコンテンツ鍵の暗号化に用いられることとなる暗号化鍵群は、それぞれ暗号化鍵0-1K1000、1-

50

1K1000、2-1K1000となる。なお、暗号化鍵特定部306は、上述の鍵特定処理により特定した暗号化鍵それぞれに対応する、鍵情報500(図9参照)中のノードID、無効化パターン等から、鍵特定情報を作成して出力し、この鍵特定情報は暗号化装置101の暗号化鍵群格納部203に格納され、暗号化装置101によりコンテンツ等とともに光ディスク102に記録されることになる。

【0086】図16は、図15に示す暗号化鍵に対応する鍵特定情報の一例を示す図である。同図の例は、鍵情報500中のノードIDである文字列と「K」という文字と無効化パターンの文字列とを結合して、鍵特定情報を構成した例である。なお、暗号化装置101の出力部206は、図16に示した鍵特定情報を光ディスクに記録する場合には、光ディスクには暗号化鍵0-1K1000を用いた暗号化により生成された暗号化コンテンツ鍵と、暗号化鍵1-1K1000を用いた暗号化により生成された暗号化コンテンツ鍵と、暗号化鍵2-1K1000を用いた暗号化により生成された暗号化コンテンツ鍵とこの順序が識別できるような方法で記録する。

【0087】<暗号化コンテンツの復号>以下、図15に示す各暗号化鍵を用いた暗号化により生成された各暗号化コンテンツ鍵と暗号化コンテンツと図16に示す鍵特定情報とが記録された光ディスク102から、1台の復号装置103nがコンテンツを復号して再生する具体的な手順について説明する。なお、復号装置103nは、復号装置103aと同様の構成を備え、復号鍵群格納部212の内容のみが異なるので、ここでは復号装置103nの各部を図2中の符号を用いて説明する。

【0088】復号装置103nの復号鍵選定部213は、取得部211を介して光ディスク102から鍵特定情報を読み出し、復号鍵群格納部212内に保持している各復号鍵とノードとの対応を示す情報、例えば、鍵情報500中の各復号鍵に対応するノードID及び無効化パターンなる情報と、その鍵特定情報を照合することにより、鍵特定情報で特定される暗号化鍵と、同一のノードについての同一の無効化パターンに対応する復号鍵、即ちその暗号化鍵に呼応する復号鍵を選定し、その復号鍵を復号鍵群格納部212中から取り出して鍵復号部214に与える。これを受け、鍵復号部214は、取得部211を介して取得されたその暗号化鍵で暗号化された暗号化コンテンツ鍵を、その復号鍵を用いて復号する。このような手順により、例えば、復号装置103nの復号鍵群格納部212内に復号鍵0-1K1000が含まれていれば、復号装置103nは、図16に示す鍵特定情報が記録された光ディスク102中における、暗号化鍵0-1K1000を用いて暗号化されたコンテンツ鍵を、その復号鍵0-1K1000を用いて復号しコンテンツ鍵を得ることになる。

【0089】コンテンツ鍵を得た後には、復号装置10

3nは、コンテンツ復号部215において、そのコンテンツ鍵を用いて、取得部211を介して取得された暗号化コンテンツを復号してコンテンツを得て、再生部216においてそのコンテンツを再生する。なお、図15における端末1が復号装置103aであるとした場合に、復号装置103aは、図11に示される22個の復号鍵しか保持しておらず、0-1K1000、1-1K1000及び2-1K1000のいずれの復号鍵も保持していないため、図15に示す各暗号化鍵を用いた暗号化により生成され光ディスク102に記録された各暗号化コンテンツ鍵を正しく復号することができず、このため光ディスク102に記録されている暗号化コンテンツを正しく復号することができず、コンテンツの再生が行えない。

【0090】<考察>データ保護システム100では、復号装置の数を約10億台(=4¹⁵台)とした場合には、レベル0からレベル15までの階層からなる4分木の木構造が構築される必要がある。この場合に、1台の復号装置を無効化端末としたとすれば、暗号化鍵特定部306による鍵特定処理において、その1台の無効化端末に対応するリーフからルートに至る経路上に存在する、リーフを除く全15個の各ノードについての1つの無効化パターンに対応する暗号化鍵が特定されることになり、この結果として、暗号化装置101においてコンテンツ鍵を暗号化するために15個の暗号化鍵が用いられる事になる。このとき、光ディスク102には、暗号化コンテンツと15個の暗号化コンテンツ鍵と鍵特定情報とが記録されることになる。

【0091】また、例えば、この約10億台の復号装置中の約1万6000台(=4⁷台)の復号装置を無効化端末としたとすれば、暗号化装置101においてコンテンツ鍵を暗号化するために、約13万1072個(4⁷×(15-7)個)の暗号化鍵が用いられることとなる。このとき、光ディスク102には、暗号化コンテンツと約13万1072個の暗号化コンテンツ鍵と鍵特定情報とが記録されることになる。

【0092】1個の暗号化コンテンツ鍵を64ビット、即ち8バイト(Byte)とすれば、約13万1072個分の暗号化コンテンツ鍵は、全部で約1メガバイト(MB)となる。従って、暗号化コンテンツ鍵の全データ量は、一般的な光ディスクの容量に対して十分に小さいデータ量であると言える。以下、本実施の形態以外の方法を用いて暗号化を行った場合における暗号化コンテンツ鍵の全データ量について検討する。

(1) 暗号化コンテンツ鍵が8バイトであり、復号装置の数を約10億台として約1万6000台の復号装置を無効化端末とするという前提の下で、仮に全ての復号装置が異なる1つの復号鍵を保持させておいて、無効化端末以外の全ての復号装置それぞれが保持している復号鍵に呼応する各暗号化鍵を用いてコンテンツ鍵を暗号化し

て光ディスクに記録して配布する方式を採用したならば、光ディスクに記録すべき暗号化コンテンツ鍵の総数は約9億9998万4000個となり、その暗号化コンテンツの全データ量は約7600メガバイトという大きなものとなってしまい、実用的でない。

(2) 同じ前提の下で、仮に、各復号装置にリーフを対応させた4分木の木構造における各ノードに1つの復号鍵のみを割り当てておき、各復号装置には、その復号装置に対応するリーフとそのリーフから上層に向けて辿ると到達できる全てのノードとのそれぞれに割り当てられている復号鍵を保持させておいて、無効化端末に対応する1つのリーフから上層に向けて辿ると到達できる全てのノード（つまり無効ノード）についての全ての子ノードのうち無効ノードでないノードそれぞれに割り当てられている暗号化鍵を用いてコンテンツ鍵を暗号化して光ディスクに記録して配布する方式を採用したならば、木構造の最下位層のレベルは15となり、光ディスクに記録すべき暗号化コンテンツ鍵の総数は約39万3216個（ $4^7 \times (15-7) \times 3$ 個）となり、その暗号化コンテンツの全データ量は約3メガバイトとなり、本実施の形態に係るデータ保護システム100による場合よりも、データ量がかなり多くなる。

(3) 同じ前提の下で、仮に、各復号装置にリーフを対応させた2分木の木構造における各ノードに1つの復号鍵のみを割り当てておき、各復号装置には、その復号装置に対応するリーフとそのリーフから上層に向けて辿ると到達できる全てのノードとのそれぞれに割り当てられている復号鍵を保持させておいて、無効化端末に対応する1つのリーフから上層に向けて辿ると到達できる全てのノード（つまり無効ノード）についての全ての子ノードのうち無効ノードでないノードそれぞれに割り当てられている暗号化鍵を用いてコンテンツ鍵を暗号化して光ディスクに記録して配布する方式を採用したならば、木構造の最下位層のレベルは30となり光ディスクに記録すべき暗号化コンテンツ鍵の総数は約26万2144個（ $2^{14} \times (30-14)$ 個）となり、その暗号化コンテンツの全データ量は約2メガバイトとなり、本実施の形態に係るデータ保護システム100による場合よりも、データ量がかなり多くなる。

＜実施の形態2＞以下、本発明の実施の形態2に係るデータ保護システム（以下、「第2データ保護システム」という。）について図を用いて説明する。

【0093】第2データ保護システムでは、復号鍵及び暗号化鍵の決定に用いるための木構造を複数個用いている点が、データ保護システム100と異なる点である。第2データ保護システムは、実施の形態1で示したデータ保護システム100と基本的に同じ構成要素（図1～図3参照）を備える。従って、ここでは第2データ保護システムの構成要素についても図1～図3に示した符号を用いて説明する。なお、ここでは、第2データ保護シ

ステムについて、データ保護システム100と異なる点を中心に説明し、同様である点についての説明は省略する。

【0094】第2データ保護システムにおける鍵情報生成部302、鍵情報更新部304、復号鍵決定部305及び暗号化鍵特定部306の具体的動作内容はデータ保護システム100中の対応する各部と異なるが、各部の行う基本となる処理内容（図10、図12、図13に示した手順等）は、ほとんど同じであり、第2データ保護

10 システムにおける鍵情報格納部301には最下位層以外の各ノードに、実施の形態1において図9で示した11種類の無効化パターンとともに11組の復号鍵及び暗号化鍵が対応付けられ、最下位層の各ノードには1組の復号鍵及び暗号化鍵が対応付けられて記憶されている。

【0095】第2データ保護システムにおける鍵設定システム104においては、鍵情報生成部302により、図17に示すような、4分木の木構造を4つ構築し、4つの木構造における全リーフのそれぞれを、復号装置103a～103nそれぞれと対応させる。従って、4つのルート1301～1304が存在し、各復号装置はいずれかの木構造のリーフに対応する。

【0096】図17は、実施の形態2に係る第2データ保護システムにおいて復号装置数が64台である場合に構築される4つの4分木の木構造の例を示す図である。この場合において、リーフが64個存在するように4つの4分木の木構造が構築されるため、最下位層はレベル2となる。例えば、第2データ保護システムにおける復号鍵決定部305の鍵割当処理により（図10参照）、図17に示した端末1に割り当てられ、最終的に端末130に保持されることになる復号鍵群は、レベル2の相対番号1のリーフに割り当てられている復号鍵2-1Kと、そのリーフの親ノードであるレベル1の相対番号1のノードについて割り当てられている復号鍵のうち、1番目の子ノードが無効ノードでないことを示す無効化パターンに対応する復号鍵、即ち"0000"、"0001"、"0010"、"0011"、"0100"、"0101"及び"0110"という7つの無効化パターンに対応する7つの復号鍵1-1K0000、1-1K0001、1-1K0010、1-1K0011、1-1K0100、1-1K0101及び1-1K0110

40 と、そのさらに1層上の親ノードであるレベル0の相対番号1のノード即ちルート1301について割り当てられている復号鍵のうち、1番目の子ノードが無効ノードでないことを示す無効化パターンに対応する7つの復号鍵0-1K0000、0-1K0001、0-1K0010、0-1K0011、0-1K0100、0-1K0101及び0-1K0110との合計15個の復号鍵である。

【0097】また例えば、第2データ保護システムにおける復号鍵決定部305により、図17に示した端末1

7に割り当てられ、端末17に保持されることになる復号鍵は、レベル2の相対番号17のリーフに割り当てられている復号鍵2-17Kと、そのリーフの親ノードであるレベル1の相対番号5のノードについて割り当てられている復号鍵のうち、1番目の子ノードが無効ノードでないことを示す無効化パターンに対応する復号鍵、即ち"0000"、"0001"、"0010"、"0011"、"0100"、"0101"及び"0110"という7つの無効化パターンに対応する7つの復号鍵1-5K0000、1-5K0001、1-5K0010、1-5K0011、1-5K0100、1-5K0101及び1-5K0110と、そのさらに1層上の親ノードであるレベル0の相対番号1のノード即ちルート1302について割り当てられている復号鍵のうち、1番目の子ノードが無効ノードでないことを示す無効化パターンに対応する7つの復号鍵0-2K0000、0-2K0001、0-2K0010、0-2K0011、0-2K0100、0-2K0101及び0-2K0110との合計15個の復号鍵である。

【0098】また、図17に示すように、無効化端末がない状態において第2データ保護システムにおける暗号化鍵特定部306により特定され(図13参照)、暗号化装置101に設定され光ディスク102へコンテンツ鍵を暗号化して記録する際に用いられる暗号化鍵は、暗号化鍵0-1K0000、0-2K0000、0-3K0000及び0-4K0000なる4つの鍵となる。

【0099】図18は、第2データ保護システムにおいて、端末1が無効化端末である状態での暗号化鍵等を示す図である。端末1のみが無効化端末であると、無効化情報更新処理(図12参照)の結果として、鍵情報格納部301に格納されている鍵情報は、レベル1の層の相対番号1番のノード1405の無効化情報が"1000"となり、レベル0の層のルート1401の無効化情報が"1000"となり、暗号化鍵特定部306により実行される鍵特定処理(図13参照)によって、暗号化装置101に設定されるべきものとして特定される暗号化鍵は、暗号化鍵0-1K1000、1-1K1000、0-2K0000、0-3K0000及び0-4K0000なる5つの鍵となる。

【0100】なお、第2データ保護システムにおける暗号化装置101及び復号装置103a～103nの動作は、実施の形態1に示したデータ保護システム100における該当装置の動作と同様である。

＜実施の形態3＞以下、本発明の実施の形態3に係るデータ保護システム(以下、「第3データ保護システム」という。)について図を用いて説明する。

【0101】第3データ保護システムは、実施の形態1及び2で示した無効化パターンとは異なる内容の無効化パターンを用いる点に特徴があるが、その他の点は基本的にデータ保護システム100と変わりない。第3デー

タ保護システムは、実施の形態1で示したデータ保護システム100と基本的に同じ構成要素(図1～図3参照)を備える。従って、ここでは第3データ保護システムの構成要素についても図1～図3に示した符号を用いて説明する。なお、ここでは、第3データ保護システムについて、データ保護システム100と異なる点を中心に説明し、同様である点についての説明は省略する。

【0102】第3データ保護システムにおける鍵情報格納部301には、最下位層以外の各ノードについて、無効化パターンとともに5組の復号鍵及び暗号化鍵が対応付けられ、最下位層の各ノードには1組の復号鍵及び暗号化鍵が対応付けられて記憶されている。但し、実施の形態1及び2においては、あるノードについての無効化情報のとり得る"0000"、"1000"等の値のうち、"1"の数がn分木の木構造である場合における(n-1)個未満となる値を無効化パターンと称することとしたが、実施の形態3における無効化パターンとは、あるノードについての無効化情報のとり得る値のうち、"1"の数が2個未満となる各値をいうこととする。

【0103】従って、無効化パターンは、"0000"、"0001"、"0010"、"0100"及び"1000"の5種類存在し、鍵情報生成部302により、リーフ以外の各ノードには、全無効化パターン分の5組の暗号化鍵及び復号鍵が対応付けられ、リーフには1組の暗号化鍵及び復号鍵が対応付けられてなる鍵情報が生成され、鍵情報格納部301に格納される。

【0104】図19は、実施の形態3において用いられる4分木の木構造における各ノードに割り当てられている復号鍵を示す図である。同図に示すように、例えばルートには0-1K0000、0-1K0001、0-1K0010、0-1K0100及び0-1K1000の5つの復号鍵が割り当てられており、レベル1の相対番号1のノードには、1-1K0000、1-1K0001、1-1K0010、1-1K0100及び1-1K1000の5つの復号鍵が割り当てられている。

【0105】以下、64台しか復号装置がない場合を例にして、第3データ保護システムの動作について説明する。図20は、64台しか復号装置がないと仮定した場合においてレベル3の相対番号1のリーフに対応する復号装置(端末1)に割り当てられる復号鍵群1705を示す図である。

【0106】第3データ保護システムにおける復号鍵決定部305の鍵割当処理(図10参照)により、図20に示した端末1に割り当てられ、最終的に端末1に保持されることになる復号鍵群1705は、レベル3の相対番号1のリーフ1704に割り当てられている復号鍵3-1Kと、そのリーフの親ノードであるレベル2の相対番号1のノード1703について割り当てられている復号鍵のうち、1番目の子ノードが無効ノードでないこと

を示す無効化パターンに対応する復号鍵、即ち" 0000 "、" 0001 "、" 0010 "及び" 0100 "という4つの無効化パターンに対応する4つの復号鍵2-1K0000、2-1K0001、2-1K0010及び2-1K0100と、その1層上の親ノードであるレベル1の相対番号1のノード1702について割り当てられている復号鍵のうち、1番目の子ノードが無効ノードでないことを示す無効化パターンに対応する4つの復号鍵1-1K0000、1-1K0001、1-1K0010及び1-1K0100と、そのさらに1層上の親ノードであるレベル0の相対番号1のノード即ちルート1701について割り当てられている復号鍵のうち、1番目の子ノードが無効ノードでないことを示す無効化パターンに対応する4つの復号鍵0-1K0000、0-1K0001、0-1K0010及び0-1K0100との合計13個の復号鍵である。従って、第3データ保護システムによれば実施の形態1で示したデータ保護システム100においてより各端末が保持する復号鍵の数は少なくて済む。

【0107】なお、復号鍵決定部305により各端末に割り当てられた復号鍵群は、各端末の製造工程等において各端末の復号鍵群格納部212に格納される。以下、第3データ保護システムの運用段階において光ディスク102へのコンテンツ等の記録に際して必要とされる暗号化鍵について説明する。64台しか復号装置がないと仮定した場合において、無効化端末がない状態では、第3データ保護システムにおける暗号化鍵特定部306の鍵特定処理により特定され、暗号化装置101の暗号化鍵群格納部203に格納され、コンテンツの光ディスク102への記録に際してコンテンツ鍵の暗号化に用いられることとなる暗号化鍵は、暗号化鍵0-1K0000、つまり復号鍵0-1K0000に呼応する1つの暗号化鍵となる。

【0108】図21は、64台しか復号装置がないと仮定した場合において、端末1、端末2及び端末17が無効化端末である状態での暗号化鍵等を示す図である。第3データ保護システムにおける鍵情報更新部304の無効化情報更新処理により(図12参照)、鍵情報格納部301内の鍵情報が更新される。なお、無効化情報更新処理は、実施の形態1で示したデータ保護システム100の鍵情報更新部304により行われる内容と全く同一である。この結果、鍵情報格納部301に格納されている鍵情報については、レベル3の層の相対番号1番、2番及び17番のリーフについての無効化情報が" 1111 "となり、レベル2の層の相対番号1番のノード1806の無効化情報が" 1100 "となり、レベル2の層の相対番号5番のノード1807の無効化情報が" 1000 "となり、レベル1の層の相対番号1番のノード1802の無効化情報が" 1000 "となり、レベル1の層の相対番号2番のノード1803の無効化情報が" 1

000 "となり、レベル0の層のルート1801の無効化情報が" 1100 "となり、他のノードの無効化情報は" 0000 "となる。なお、対応する無効化情報が" 0000 "のノードが有効ノードであり、それ以外のノードが、無効ノードである。

【0109】無効化情報更新処理に続いて暗号化鍵特定部306の鍵特定処理(図13参照)により暗号化鍵の特定が行われる。以下、図21に示す例に基づく鍵特定処理の具体的な処理内容を図13を用いて説明する。この例においては、最下位層はレベル3となる。

【0110】まず、暗号化鍵特定部306は、最上位層のノード、即ちルート1801に着目する(ステップS31)。続いて暗号化鍵特定部306は、着目しているノード1801について、鍵情報格納部301に格納されている鍵情報を参照して、そのノード1801の無効化情報である" 1100 "が、上述した5種類の無効化パターンのいずれかと合致するかを判定し(ステップS32)、いずれとも合致しないので、次に着目しているノード1801の1層だけ下の層は最下位層であるかを判定し(ステップS36)、着目しているノード1801の1層だけ下の層はレベル1の層であり最下位層ではないため、ノード1801の全ての子ノードを着目予定ノードと定める(ステップS38)。

【0111】このステップS38により、ノード1802-1805が着目予定ノードとなる。続いて、暗号化鍵特定部306は、未着目の着目予定ノードがあるか判定し(ステップS39)、未着目の着目予定が存在するのでその1つであるノード1802に着目し(ステップS40)、ステップS32の判定処理に戻って、鍵情報を参照して、着目しているノード1802の無効化情報である" 1000 "が、上述した5種類の無効化パターンのいずれかと合致するかを判定し(ステップS32)、合致するのでノード1802についての無効化パターン" 1000 "に対応する暗号化鍵1-1K1000を暗号化装置101に設定すべき暗号化鍵として特定し(ステップS33)、着目しているノード1802の1層下の層はレベル2の層であり最下位層ではないため(ステップS34)、ノード1802の子ノードのうち無効ノードであるノード1806を着目予定ノードと定める(ステップS35)。

【0112】ステップS35の後、暗号化鍵特定部306は、未着目の着目予定ノードがあるか判定し(ステップS39)、未着目の着目予定が存在するのでその1つであるノード1806に着目し(ステップS40)、ステップS32の判定処理に戻る。次に、暗号化鍵特定部306は、鍵情報を参照してノード1806の無効化情報である" 1100 "が、上述した5種類の無効化パターンのいずれかと合致するかを判定し(ステップS32)、いずれとも合致しないので、次に着目しているノード1806の1層だけ下の層は最下位層であるかを判

定し(ステップS36)、ノード1806の1層だけ下の層はレベル3の層であり最下位層であるため、そのノード1806の子ノードのうちの有効ノードであるリーフ1808、1809それぞれに対応する暗号化鍵3-3K、暗号化鍵3-4Kを暗号化装置101に設定すべき暗号化鍵として特定し(ステップS37)、未着目の着目予定ノードがあるか判定し(ステップS39)、未着目の着目予定が存在するのでその1つであるノード1803に着目し(ステップS40)、ステップS32の判定処理に戻る。

【0113】次に、暗号化鍵特定部306は、鍵情報を参照してノード1803の無効化情報である"1000"が、上述した5種類の無効化パターンのいずれかと合致するかを判定し(ステップS32)、合致するのでノード1803についての無効化パターン"1000"に対応する暗号化鍵1-2K1000を暗号化装置101に設定すべき暗号化鍵として特定し(ステップS33)、着目しているノード1803の1層下の層はレベル2の層であり最下位層ではないため(ステップS34)、ノード1803の子ノードのうち無効ノードであるノード1807を着目予定ノードと定める(ステップS35)。

【0114】続いて、暗号化鍵特定部306は、未着目の着目予定ノードがあるか判定し(ステップS39)、未着目の着目予定が存在するのでその1つであるノード1807に着目し(ステップS40)、ステップS32の判定処理に戻って、鍵情報を参照して、着目しているノード1807の無効化情報である"1000"が、上述した5種類の無効化パターンのいずれかと合致するかを判定し(ステップS32)、合致するのでノード1807についての無効化パターン"1000"に対応する暗号化鍵2-5K1000を暗号化装置101に設定すべき暗号化鍵として特定し(ステップS33)、着目しているノード1807の1層下の層はレベル3の層であり最下位層であるため(ステップS34)、ステップS35の処理をスキップして、未着目の着目予定ノードがあるか判定し(ステップS39)、未着目の着目予定が存在するのでその1つであるノード1804に着目し(ステップS40)、ステップS32の判定処理に戻る。

【0115】次に、暗号化鍵特定部306は、鍵情報を参照して、着目しているノード1804の無効化情報である"0000"が、上述した5種類の無効化パターンのいずれかと合致するかを判定し(ステップS32)、合致するのでノード1804についての無効化パターン"0000"に対応する暗号化鍵1-3K0000を暗号化装置101に設定すべき暗号化鍵として特定し(ステップS33)、着目しているノード1804の1層下の層はレベル2の層であり最下位層ではないため(ステップS34)、ノード1804の子ノードのうち

無効ノードを着目予定ノードと定めようとする(ステップS35)。しかし、ノード1804の子ノードは全て有効ノードなので新たに着目予定ノードは定められない。

【0116】続いて、暗号化鍵特定部306は、未着目の着目予定ノードがあるか判定し(ステップS39)、未着目の着目予定ノードであるノード1805に着目し(ステップS40)、ステップS32の判定処理に戻り、鍵情報を参照して、着目しているノード1805の無効化情報である"0000"が、上述した5種類の無効化パターンのいずれかと合致するかを判定し(ステップS32)、合致するのでノード1805についての無効化パターン"0000"に対応する暗号化鍵1-4K0000を暗号化装置101に設定すべき暗号化鍵として特定し(ステップS33)、着目しているノード1805の1層下の層はレベル2の層であり最下位層ではないため(ステップS34)、ノード1805の子ノードのうち無効ノードを着目予定ノードと定めようとする(ステップS35)。しかし、ノード1805の子ノードは全て有効ノードなので新たに着目予定ノードは定められない。

【0117】続いて、暗号化鍵特定部306は、未着目の着目予定ノードがあるか判定し(ステップS39)、未着目の着目予定ノードはもう存在しないので、鍵特定処理を終える。このような鍵特定処理の結果として、暗号化装置101に設定すべきものとして特定された暗号化鍵は、暗号化鍵1-1K1000、1-2K1000、1-3K0000、1-4K0000、2-5K1000、3-3K及び3-4Kなる7個の鍵である。

【0118】なお、この7個の暗号化鍵は、後に暗号化装置101の暗号化鍵群格納部203に格納され、鍵暗号化部204によりコンテンツ鍵の暗号化に用いられる。また、各暗号化鍵を用いた暗号化により生成された各暗号化コンテンツ鍵が、出力部206により、各暗号化鍵に呼応する復号鍵を特定するために用いることできる鍵特定情報と暗号化コンテンツとともに光ディスク102に記録されることになる。

【0119】上述の復号鍵決定部305による各端末への復号鍵の割当の結果として、この7個の暗号化鍵に呼応する復号鍵はいずれも、端末1、端末2或いは端末7に保持されておらず、また、この7個の暗号化鍵に呼応する復号鍵のうちいずれか1つ以上が、その他の端末には保持されている。従って、この7つの暗号化鍵を用いた暗号化処理によりコンテンツが光ディスク102に記録された後においては、端末1、端末2及び端末7から暴露された復号鍵を用いてその光ディスク102に記録されたコンテンツの復号処理を正常に行うことはできず、また、他の端末では光ディスク102に記録されたコンテンツの復号処理を正常に行うことができるようになる。

<実施の形態4>以下、本発明の実施の形態4に係るデータ保護システム（以下、「第4データ保護システム」という。）について図を用いて説明する。

【0120】実施の形態1で示したデータ保護システム100において、暗号化装置101が暗号化コンテンツを記録して各復号装置103a～103nに配給するための光ディスク102は、DVD-ROM等であることとしたが、第4データ保護システムは、光ディスク102を、DVD-ROM等のいわゆるプレレコーディッドメディアと、DVD-RAM等のいわゆるレコーダブルメディアとに2分した場合におけるレコーダブルメディアのみを前提とした実施の形態である。

【0121】即ち、第4データ保護システムは、レコーダブルメディアである光ディスク102に対して、システム側において一定の情報を記録しておき、ユーザが端末により任意のコンテンツをその光ディスク102に対して暗号化して記録して、光ディスク102を配布することができ、また同一又は別の端末においてユーザが光ディスク102に記録されているコンテンツを復号して利用できるようにしたシステムである。なお、ここでは、第4データ保護システムについて、データ保護システム100と異なる点を中心に説明し、同様である点についての説明は省略する。

【0122】図22は、本発明の実施の形態4に係る第4データ保護システムの概略構成図である。第4データ保護システムは、同図に示すように、鍵特定情報記録装置1501、複数のユーザデータ暗号化装置（端末）1502a～1502n、複数の復号装置（端末）103a～103n及び鍵設定システム104を備える。例えば、鍵設定システム104及び鍵特定情報記録装置1501は著作権保護の管理を行う機関に運用され、各端末は一般ユーザに利用されることが想定される。

【0123】なお、復号装置103a～103nは実施の形態1で示したものと同一であり、また、ユーザデータ暗号化装置1502a～1502nの全部又は一部は復号装置103a～103nの全部又は一部と同一の端末に実装されることとしてもよい。また、第4データ保護システムにおける鍵設定システム104は実施の形態1で示したものと基本的に同一であるが、若干の機能追加がある。即ち、第4データ保護システムにおける鍵設定システム104は、予め各端末をリーフに対応させた4分木の木構造の構築を前提として、図10に示す鍵割当処理により各端末に復号鍵群を割り当てるが、この際に、割当対象の端末が復号装置であれば復号鍵群を割り当て、割当対象の端末がユーザデータ暗号化装置であればその復号鍵群に呼応する暗号化鍵群を割り当てるものとする。なお、鍵設定システム104は、各端末に対して割り当てた鍵と木構造におけるノードとの対応を示す情報を生成して出力する。

【0124】この実施の形態4においては、便宜上、ユ

ーザデータ暗号化装置1502a～1502nがそれぞれ、復号装置103a～103nのそれぞれと同一端末に実装されているものとし、また、呼応する暗号化鍵と復号鍵は同一値であることとして説明する。従って、予め各端末には鍵設定システム104により割り当てられた復号鍵群でありかつ暗号化鍵群である鍵群と、その各鍵と木構造におけるノードとの対応を示す情報を鍵設定システム104から取得して保持する。

【0125】また、第4データ保護システムにおける鍵設定システム104は更に、運用段階において無効化情報更新処理（図12参照）及び鍵特定処理（図13参照）の結果として特定された1又は複数の暗号化鍵を指示する鍵特定情報（図16参照）を、鍵特定情報記録装置1501に出力する機能を有する。例えば、無効化端末がない状態では、鍵特定情報は、「0-1K0000」のみとなる。

【0126】鍵特定情報記録装置1501は、データを光ディスクに記録可能なハードウェアを含み、鍵設定システム104から入力された鍵特定情報を光ディスク102に記録する機能を有する装置である。また、ユーザデータ暗号化装置1502a～1502nそれぞれは、実施の形態1で示した暗号化装置101（図2参照）の各機能に相当する機能を備える。但し、コンテンツ記憶部201にはユーザが自由にデジタルコンテンツを格納することができ、暗号化鍵格納部203の内容は、上述した鍵設定システム104から取得して端末が保持している暗号化鍵群と、各暗号化鍵と木構造におけるノードとの対応を示す情報であり、鍵暗号化部204が乱数発生部202から取得したコンテンツ鍵の暗号化に用いる暗号化鍵は、後述する暗号化鍵選定処理の結果として選定されたものであり、また、出力部206は、鍵特定情報を光ディスク102に記録せず、暗号化コンテンツ及び暗号化コンテンツ鍵を光ディスク102に記録する。

【0127】また、ユーザデータ暗号化装置1502a～1502nそれぞれは、更に光ディスク102から鍵特定情報記録装置1501によって記録された鍵特定情報を読み出してコンテンツ鍵の暗号化に用いる暗号化鍵を選定する暗号化鍵選定処理を行う機能を有する。この暗号化鍵選定処理は、暗号化鍵格納部203内の各暗号化鍵とノードとの対応を示す情報と鍵特定情報を照合して、両者に同じノードを示す内容があればそのノードに対応する暗号化鍵を選定して鍵暗号化部204に送出する処理であり、実施の形態1で示した復号装置103a中の復号鍵選定部213における復号鍵を選定する処理と同様の処理である。

【0128】即ち、ユーザデータ暗号化装置1502a～1502nそれぞれは、光ディスク102にコンテンツをコンテンツ鍵で暗号化して記録する場合において、光ディスク102内に予め記録されている鍵特定情報に

従った暗号化鍵を用いてコンテンツ鍵を暗号化して光ディスク102に記録する機能を有する装置である。従って、この第4データ保護システムによれば、不正に解析される等して復号鍵等が暴露された端末以外の多数の端末において、暴露された復号鍵によっては正しく復号できず、暴露されていない復号鍵を持つ多数の端末では正しく復号して利用できるようにコンテンツを暗号化して光ディスク102に記録することができるようになる。<補足>以上、本発明に係るデータ保護システムについて、実施の形態1～4に基づいて説明したが、本発明はこれらの実施の形態に限られないことは勿論である。即ち、

(1) 実施の形態1～4で示したコンテンツは映像、音声等であることとしたが、コンテンツの内容はこれらに限定されることはなく、プログラムその他のデータであっても、これらと映像等との組み合わせであってもよい。

(2) 実施の形態1～4で示した復号装置は、復号したコンテンツを再生する再生部216を備えることとしたが、その代わりに復号したコンテンツを装置外部に出力する機能を有することとしてもよい。

(3) 実施の形態1～3では、暗号化コンテンツ等を光ディスク102に記録して各復号装置に配布する形態を示したが、暗号化コンテンツ等を各復号装置に配給する形態として、記録媒体による配布の他に、無線又は有線の伝送路を通じて配信するという形態としてもよい。

【0129】暗号化コンテンツ等を配信する形態を採用する場合においては、暗号化装置101の出力部206は、通信機能を有するハードウェアを備えるものとし、暗号化コンテンツ、暗号化コンテンツ鍵及び鍵特定情報を各復号装置（端末）に送信することとする必要があり、復号装置103a等の取得部211は、通信機能を有するハードウェアを備えるものとし、暗号化コンテンツ、暗号化コンテンツ鍵及び鍵特定情報を受信して取得することとする必要がある。なお、配信の方法としては、例えば、暗号化装置101が例えばインターネットに接続されているサーバ中の記録媒体に記録し復号装置103a等がその記録媒体の内容をインターネットを通じて受信することとしてもよい。

【0130】また、暗号化コンテンツ等を記録媒体に記録して配布する形態を採用する場合における記録媒体は、光ディスクに限られることはなく、ICカード、フレキシブルディスク、磁気テープ、ROM等であってもよい。

(4) 実施の形態1で示した鍵情報における各ノードに対応する無効化パターンの定め方は、単なる一例であり、例えばルート以外の各ノードが“0000”という無効化パターンを持たないこととし、リーフ以外の各ノードが“0111”、“1101”、“1011”、“1110”という無効化パターンを持つこととして、こ

れに合わせて鍵割当処理（図10参照）及び鍵特定処理（図13参照）の内容を若干変更することとしてもよい。

【0131】また、実施の形態1等では4分木の木構造の構築を前提として無効化パターン等を定めたが、前提となる木構造は、nが3以上であるn分木の木構造を少なくとも一部に含む木構造、つまり少なくとも一層における1のノードが3以上の子ノードの親ノードであるような木構造であればよく、3分木であっても、5分木であってもよく、各層において3分木や4分木等が異なるような木構造を用いることとしてもよい。

【0132】また、実施の形態1では、4分木の木構造の各ノードについての無効化パターンは「1」の数が3未満のものに限ることとしており、実施の形態3では、4分木の木構造の各ノードについての無効化パターンは「1」の数が2未満のものに限ることとしたが、例えば5分木の木構造の各ノードについての無効化パターンは「1」の数が2未満のものに限ることとしても、3未満のものに限ることとしても、4未満のものに限ることとしてもよい。

(5) 実施の形態1～4に示した復号装置103a～103nにおける復号に関連する各部及び実施の形態4に示したユーザデータ暗号化装置1502a～1502nにおける暗号化に関連する各部は、いわゆる耐タンパ技術により、復号又は暗号化に用いられる方式やデータが保護されるように構成されることが望ましい。

(6) 実施の形態1等で鍵設定システムは各端末に割り当てるべき復号鍵を決定した際に復号鍵と、その復号鍵が対応する木構造におけるノードを示す情報を出力し、この結果として復号装置103a～103nが復号鍵群と、各復号鍵に対応するノードを示す情報を保持することとしたが、復号装置は、必ずしも復号鍵に対応するノードを示す情報を保持する必要はない。復号鍵に対応するノードを示す情報を保持しない場合においては、光ディスクに記録されている暗号化コンテンツ鍵を、復号装置は自ら保持している各復号鍵を順次用いた復号を試みる方法により、コンテンツ鍵を復号することとしてもよい。なお、この場合、コンテンツ鍵には予め先頭8ビットが0である等の規則を設けておくことや、

一般的なデジタル署名等を用いて、復号したコンテンツ鍵の正当性が確認できるようにしておくこととし、復号装置は、復号したコンテンツ鍵が正当であるときにのみそのコンテンツ鍵を用いてコンテンツを復号するようにしてよい。

(7) 実施の形態1ではコンテンツ鍵、復号鍵及び暗号鍵は64ビットであることとしたが、鍵のデータサイズについては64ビットに限定されることなく、他のビット数であってもよい。なお、図16において、鍵特定情報がノードIDである文字列と「K」という文字と無効化パターンの文字列とを結合してなる文字列を含む

こととしたが、鍵特定情報のフォーマットはこれに限定されることはない。

(8) 実施の形態1～4では、コンテンツの暗号化に用いられるコンテンツ鍵を、0-1K0000等で表される暗号化鍵を用いた暗号化の対象としたが、暗号化の対象は、コンテンツ鍵に限定されることはなく、機密保持を要するいかなるデータであってもよい。

(9) 実施の形態1～4に示した鍵設定システム104における無効化情報更新処理、鍵割当処理又は鍵特定処理(図10、図12又は図13に示した手順等)をコンピュータ又はプログラム実行機能を備える機器に実行させるためのコンピュータプログラムを、記録媒体に記録し又は各種通信路等を介して、流通させ頒布することもできる。このような記録媒体には、ICカード、光ディスク、フレキシブルディスク、ROM等がある。流通、頒布されたコンピュータプログラムはコンピュータ等にインストールされることにより利用に供され、コンピュータ等はそのコンピュータプログラムの実行により実施の形態1～4で示したような無効化情報更新処理、鍵割当処理又は鍵特定処理を行う。

【0133】

【発明の効果】以上説明したことから明らかなように、本発明に係るデータ保護システムは、3台以上の端末、暗号化装置及び暗号化鍵特定装置を備え、各端末への配給用データを暗号化装置により暗号化して保護するデータ保護システムであって、前記各端末は、所定鍵割当方法により個別に割当てられた復号鍵群を記憶しており、前記暗号化装置から出力された暗号化配給用データ群を取得して、暗号化配給用データを、記憶している復号鍵を用いて復号するものであり、前記所定鍵割当方法は、(a)前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいづれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定し、(b)端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c)前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であり、前記暗号化鍵特定装置は、暗号化鍵を特定する装置であり、かつ、1つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記所定鍵割当方法により端末に割当てられた全ての復号鍵のうち無効化端末に割当てられた復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が割り当てられていない最も多くの端末に、割当てられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が割り当てられていない端末が存在しなくなるま

で繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを有する装置であり、前記暗号化装置は、前記暗号化鍵特定装置により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成して出力する暗号化手段を有することを特徴とする。

【0134】ここで、配給用データは、記録媒体に記録されて配布され、或いは有線又は無線の通信路を通じて配信され、最終的に各端末に到達することが想定されるデータである。端末1、端末2、端末3を想定すれば、

10 上述の所定鍵割当方法により決定される端末集合には、端末1及び端末2の組Aや、端末1及び端末3の組Bや、端末2及び端末3の組Cがあり、所定鍵割当方法による割り当て結果を受けて端末1が記憶保持する復号鍵は端末1固有の復号鍵と、組Aに対応する復号鍵Aと、組Bに対応する復号鍵Bとであり、端末2が記憶保持する復号鍵は端末2固有の復号鍵と、組Aに対応する復号鍵Aと、組Cに対応する復号鍵Cとであり、端末3が記憶保持する復号鍵は端末3固有の復号鍵と、組Bに対応する復号鍵Bと、組Cに対応する復号鍵Cとである。この例において、端末2が不正に解析等されて端末2が記憶保持する全ての復号鍵が暴露されてしまった場合には端末2を無効化端末、つまり無効化にすべき端末として特定し、前記暗号化鍵特定手段による暗号化鍵の特定を行うと復号鍵Bに呼応する暗号化鍵が特定されることになる。

【0135】従って、復号鍵Bに呼応する暗号化鍵を用いてデータを暗号化して各端末に配給すれば、端末2では正しくそのデータを復号することができず、端末1及び端末3では正しくそのデータを復号することができる。同様の目的を、端末1固有の復号鍵に呼応する暗号化鍵と端末3固有の復号鍵に呼応する暗号化鍵とをそれぞれ用いてデータを暗号化して各端末に配給することができるが、この方法と比べて前述の復号鍵Bに呼応する暗号化鍵を用いる方法は、暗号化に用いる暗号化鍵の数が少なく、その分だけ配給される暗号化データのデータ量が少なくなるという効果を有する。

【0136】即ち、本発明によれば、暗号化したデジタルコンテンツの復号に必要な鍵等のデータを暗号化して同一データを複数の端末に配給するデータ保護システムにおいて、配給対象の暗号化データの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合に、その特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるようにすることが可能となる。

【0137】また、前記所定鍵割当方法は更に、前記複数の端末集合を完全に包含する端末集合が存在するよう50 に、かつ、同じ1つ以上の端末集合を各々包含する複数

の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、端末集合の前記決定を行う方法であることとしてもよい。

【0138】例えれば、端末集合A及び端末集合Bを包含する端末集合ABには復号鍵ABが、端末集合B及び端末集合Cを包含する端末集合BCには復号鍵BCが対応付けられている場合について言えば、このデータ保護システムにおいては、端末集合Aに属するが端末集合Bにも端末集合Cにも属さない端末には、少なくとも復号鍵ABが割り当てられ記憶保持されるが復号鍵BCは割り当てられず記憶保持されず、端末集合B又は端末集合Cに属する端末には少なくとも復号鍵BCが割り当てられる。従って、端末集合Aに属するが端末集合Bにも端末集合Cにも属さない端末が不正に解析等された後においても、少なくとも復号鍵BCに呼応する暗号化鍵を用いてデータを暗号化して各端末に配給することにより、端末集合BCに包含される端末群即ち端末集合Bに包含される端末群及び端末集合Cに包含される端末群が復号鍵BCを用いてデータを正しく復号することができるようになり、少ない暗号化鍵を用いて多くの端末で正しく復号できるようにデータを暗号化することが可能になる。

【0139】また、前記所定鍵割当方法は更に、各端末集合が3台以上の端末を要素に含むように、かつ、3台以上の端末集合を包含する端末集合が存在するように、端末集合の前記決定を行う方法であることとしてもよい。これにより、暗号化済みの同一データを各端末に配給する際において、3台以上の端末に共通な鍵を用いた暗号化が行えるので、各々別個な鍵を用いた場合よりも配給対象のデータ量を削減することができるようになる。

【0140】また、前記データ保護システムは、各端末を各々別個の最下位層のノードに対応させた複数階層のN分木（Nは3以上の自然数）の木構造を想定した場合における最下位層を除く各ノードについて、当該ノード（親ノード）から辿り着く1段下位層のN個のノードのうち、2以上を組合せてなりN個全部の組合せを含む複数の組合せパターンを決定し、決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶しており、更に最下位層の各ノードに対応付けて別個の復号鍵を記憶している鍵記憶装置と、前記所定鍵割当方法を実行し、前記各端末に割り当てる復号鍵群を決定する装置であり、かつ、前記各端末について、当該端末に対応する最下位層のノードから最上位層のノードまでの経路上に位置する最下位層でない各ノードについて、当該ノードに対応付けて前記鍵記憶装置により記憶されている復号鍵のうち、当該ノードの1段下位層で当該経路上に位置するノードを含む組合せに係る全ての前記組合せパターンに対

応する復号鍵と、当該端末に対応付けて前記鍵記憶装置により記憶されている復号鍵とを、当該端末に割り当てるべきものとして決定する復号鍵決定装置とを備え、前記各端末集合は、前記各組合せパターンと一对一に対応し、対応する組合せパターンにおいて組み合わされた全ノードから辿り着く最下位層のノードに対応する全ての端末を要素とする集合に相当するものであり、前記暗号化鍵特定手段は、前記木構造を想定した場合において、いずれかの無効化端末に対応する最下位層のノードに辿り着く全てのノードを無効ノードと定め、まず最上位層ノードを処理対象ノードとしておき、未処理の処理対象ノードが存在しなくなるまで暗号化鍵特定処理を繰り返し行い、前記暗号化鍵特定処理は、未処理の1つの処理対象ノードについて、(a)当該処理対象ノードの1段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在する場合には、当該組合せパターンに対応して前記鍵記憶装置により記憶されている復号鍵に呼応する暗号化鍵を特定し、(b)当該処理対象ノードの1段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在しない場合には、当該1段下位層が最下位層であれば当該1段下位層における無効ノード以外の全てのノードに対応して前記鍵記憶装置により記憶されている復号鍵に呼応する暗号化鍵を特定し、当該1段下位層が最下位層でなければ当該1段下位層における無効ノード以外の全てのノードを新たに処理対象ノードとし、(c)当該処理対象ノードの1段下位層において無効ノードが存在すれば、当該1段階層が最下位層でない限り全ての無効ノードを新たに処理対象ノードとする処理であることとしてもよい。

【0141】このように、木構造におけるノード毎に復号鍵等の情報を対応付けておき、その情報と木構造における各ノードの位置付けに基づいて各端末に割り当てる復号鍵を決定し、配給用データの暗号化に用いる暗号化鍵を特定する方式によって、比較的容易に上述の目的、即ち配給対象の暗号化データの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合に、その特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるようにするという目的を達成するシステムが実現できる。

【0142】また、前記鍵記憶装置による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く1段下位層のN個のノードのうち、2以上を組合せてなる全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該鍵記憶装置は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることとしても

よい。

【0143】これにより、各端末への配給用データの暗号化に用いる暗号化鍵の特定をn分木の木構造を用いて行う方式の中では、特定される暗号化鍵の数が少なく抑えられるので、結果的に各端末へ配給される暗号化配給用データのデータ量を比較的小さく抑えることが可能になる。また、前記鍵記憶装置による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く1段下位層のN個のノードのうち、N個全部の組合せ及び（N-1）個の全ての組合せそれに対応するように組合せパターンを定めることによりなされ、当該鍵記憶装置は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることとしてもよい。

【0144】これにより、各端末への配給用データの暗号化に用いる暗号化鍵の特定をn分木の木構造を用いて行う方式の中では、各端末に割り当てられる復号鍵の数が比較的少なく抑えられるので、結果的に各端末が記憶保持する復号鍵群のデータ量を比較的小さく抑えることが可能になる。また、前記暗号化手段は、前記暗号化鍵特定装置により特定された全ての暗号化鍵それぞれについて、当該暗号化鍵を用いた暗号化により生成した暗号化配給用データと、前記鍵記憶装置により当該暗号化鍵に呼応する復号鍵と対応付けられていたノードの前記木構造における所在位置を特定するための暗号化鍵ノード識別情報を、対応付けて出力し、前記各端末は、所定鍵割当方法により個別に割当てられた各復号鍵を、前記鍵記憶装置により当該復号鍵と対応付けられていたノードの前記木構造における所在位置を特定するための復号鍵ノード識別情報を対応付けて記憶しており、前記暗号化装置から出力された暗号化配給用データ群及び暗号化鍵ノード識別情報群を取得して、当該端末が記憶している復号鍵ノード識別情報と一致する暗号化鍵ノード識別情報と対応する暗号化配給用データを、当該一致に係る復号鍵ノード識別情報と対応する復号鍵を用いて復号することとしてもよい。

【0145】これにより、各端末は、1以上の暗号化鍵をそれぞれ用いて配給用データが暗号化されたものである暗号化配給用データ群を取得した後、暗号化鍵ノード識別情報群を参照することにより、自端末が保持するいずれの復号鍵を用いて復号を行うとよいかを簡単に特定することが可能となり、試行錯誤的に自端末が保持する復号鍵を逐次用いて復号を行う場合に比べて、正しく復号されるまでにかかる時間が短縮される。

【0146】また、前記暗号化鍵特定装置は、前記鍵記憶装置により記憶されている各復号鍵に呼応する暗号化鍵を記憶している暗号化鍵記憶手段を有し、前記呼応する復号鍵と暗号化鍵とは互いに異なることとしてもよ

い。これにより、ある端末の不正な解析等により復号鍵が暴露された場合にも、複数の端末で正しく復号できるようデータを暗号化するための暗号化鍵が不正に知られて悪用されるような事態の発生を防止することができるようになる。

【0147】また、前記暗号化手段による前記出力は、生成した前記暗号化配給用データ群をデータ記録媒体に記録することであり、前記各端末は、前記暗号化装置により暗号化配給用データ群が記録されたデータ記録媒体

10 から当該暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号することとしてもよい。これにより、DVD-ROM等の光ディスクその他の記録媒体にデータが暗号化して記録されるので、例えばその記録媒体と同一内容の記録媒体を量産して有償又は無償で多数の人に頒布することができ、その頒布された記録媒体を受け取った人はその記録媒体を端末にセットして端末を通じて、その記録媒体に記録されているデータを利用することができるようになる。

【0148】また、前記暗号化手段は、デジタル著作物20 であるコンテンツデータを記憶しているコンテンツ記憶部と、乱数である前記配給用データを生成する乱数データ発生部と、前記乱数データ発生部により生成された配給用データを鍵として用いて前記コンテンツデータを暗号化して、暗号化コンテンツデータを生成するコンテンツ暗号化部とを有し、前記暗号化手段は、前記暗号化鍵特定装置により特定された全ての暗号化鍵を逐次用いて前記乱数データ発生部により生成された配給用データを暗号化することにより、暗号化配給用データ群を生成して、当該暗号化配給用データ群と、前記コンテンツ暗号化部により生成された暗号化コンテンツデータとを前記データ記録媒体に記録し、前記各端末は、前記データ記録媒体から暗号化コンテンツデータ及び暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号し、復号結果である配給用データを用いて、当該暗号化コンテンツデータを復号することとしてもよい。

【0149】これにより、暗号化した映像、音声等のデジタルコンテンツの復号に必要な鍵を暗号化して、暗号化したデジタルコンテンツやその暗号化した鍵を含むデータを記録媒体に記録するので、例えば、その記録媒体40 と同一内容の記録媒体が多数の人に頒布され、頒布された記録媒体を受け取った人はその記録媒体を端末にセットして端末を通じて、デジタルコンテンツの再生等を行うことができるようになる。

【0150】また、前記データ保護システムは更に、前記暗号化鍵特定装置により特定された暗号化鍵を特定するための暗号化鍵特定情報を、データ記録媒体に記録する暗号化鍵特定情報記録装置を備え、前記各端末は、乱数である前記配給用データを生成する乱数データ発生部と、デジタル著作物であるコンテンツデータを格納しているコンテンツ格納部と、前記データ記録媒体から暗号

化鍵特定情報を読み出し、当該端末に記憶されている復号鍵群に呼応する暗号化鍵群のうち当該暗号化鍵特定情報で特定される暗号化鍵を選定する暗号化鍵選定部とを有し、前記暗号化手段は、前記暗号化鍵選定部により選定された全ての暗号化鍵を逐次用いて前記乱数データ発生部により生成された配給用データを暗号化することにより暗号化配給用データ群を生成して、前記データ記録媒体に記録するものであり、前記各端末は更に、前記乱数データ発生部により生成された配給用データを鍵として用いて前記コンテンツ格納部に格納されているコンテンツデータを暗号化して、暗号化コンテンツデータを生成し、当該暗号化コンテンツデータを前記データ記録媒体に記録するコンテンツ暗号化部と、前記各端末は、前記データ記録媒体から暗号化コンテンツデータ及び暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号し、復号結果である配給用データを用いて、当該暗号化コンテンツデータを復号することとしてもよい。

【0151】これにより、DVD-RAM等の記録媒体に、端末のユーザが任意の映像、音声等のデジタルコンテンツを記録して頒布することが可能なシステムにおいて、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合に、その特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるようにデジタルコンテンツを暗号化することが可能になる。

【0152】また、前記暗号化手段による前記出力は、生成した前記暗号化配給用データ群を前記各端末に送信することであり、前記各端末は、前記暗号化装置により送信された暗号化配給用データ群を受信して取得し、暗号化配給用データを復号することとしてもよい。これにより、配給用データは暗号化され各端末に送信されることになるため、各端末においてはその受信により容易に配給用データを利用することが可能になる。

【0153】また、本発明に係る復号鍵決定装置は、暗号化されたデータを取得して復号するための3台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定装置であって、(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するよう、2つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号

10

20

30

40

50

鍵群として決定する復号鍵群割当手段とを備えることとしてもよい。

【0154】また、本発明に係る復号鍵決定方法は、暗号化されたデータを取得して復号するための3台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定方法であって、前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するよう、2つ以上の端末集合を決定する端末集合決定ステップと、端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当ステップとを含むことを特徴とする。

【0155】また、本発明に係る復号端末システムは、暗号化されたデータを取得して復号するための3台以上の端末から構成される復号端末システムであって、前記各端末は、所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、暗号化されたデータを取得する暗号化データ取得手段と、前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段とを備え、前記所定鍵割当方法は、(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するよう、2つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c) 前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする。

【0156】また、本発明に係る復号端末は、暗号化されたデータを取得して復号するための復号端末であって、所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、暗号化されたデータを取得する暗号化データ取得手段と、前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段と、前記所定鍵割当方法は、(a) 本端末を含む3台以

上の端末を想定した場合において本端末が、2つ以上の端末を要素に含む集合である複数の端末集合に属するよう、更に、本端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定し、(b) 本端末に対応して及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c) 本端末に対して、本端末に対応して定めた復号鍵、及び本端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする。

【0157】これらにより、例えば、各端末へ記録媒体に暗号化された結果のデータを記録して記録媒体を配布する場合において、その記録媒体に記録されるデータの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合にその特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるように、その暗号化を実施することが可能になる。

【0158】また、前記暗号化データ取得手段は、前記暗号化されたデータをデータ記録媒体から読み出して取得することとしてもよい。これにより、暗号化されたデータをデータ記録媒体に記録してその記録媒体を各端末のユーザーに配布することによって各端末のユーザーにデータを利用させることができになる。

【0159】また、前記データ記録媒体には、暗号化鍵を特定するための暗号化鍵特定情報が記録されており、前記端末は更に、乱数である鍵データを生成する乱数データ発生手段と、デジタル著作物であるコンテンツデータを格納しているコンテンツ格納手段と、前記データ記録媒体から暗号化鍵特定情報を読み出し、前記復号鍵群記憶手段に記憶されている復号鍵群に呼応する暗号化鍵群のうち当該暗号化鍵特定情報で特定される暗号化鍵を選定する暗号化鍵選定手段と、前記暗号化鍵選定手段により選定された全ての暗号化鍵を逐次用いて前記乱数データ発生手段により生成された鍵データを暗号化することにより暗号化鍵データ群を生成して、当該暗号化鍵データ群を前記データ記録媒体に記録する鍵データ暗号化手段と、前記乱数データ発生手段により生成された鍵データを鍵として用いて前記コンテンツ格納部に格納されているコンテンツデータを暗号化することにより暗号化コンテンツデータを生成し、当該暗号化コンテンツデータを前記データ記録媒体に記録するコンテンツ暗号化手段とを備え、前記暗号化データ取得手段は、前記データ記録媒体に記録されている暗号化鍵データ及び暗号化コンテンツデータを取得し、前記復号手段は、前記暗号化データ取得手段により取得された前記暗号化鍵データを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号することにより鍵データを生成するものであ

り、前記端末は更に、前記暗号化データ取得手段により取得された前記暗号化コンテンツデータを、前記復号手段により生成された鍵データを用いて復号するコンテンツ復号手段を備えることとしてもよい。

【0160】これにより、各端末のユーザーは、映像、音声等のデジタルコンテンツを暗号化して記録媒体に記録することができるようになる。また、前記暗号化されたデータは外部の送信装置から送信されるものであり、前記暗号化データ取得手段は、前記暗号化されたデータを受信することにより取得することとしてもよい。

【0161】これにより、デジタルコンテンツ等の送信されたデータを各端末においては受信により容易に利用することができるようになる。また、本発明に係る暗号化鍵特定装置は、3台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定する暗号化鍵特定装置であって、(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するよう、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵群対応付け手段と、前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵設定手段と、1つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを備えることを特徴とする。

【0162】また、本発明に係る暗号化装置は、3台以上の各端末への配給用データを暗号化する暗号化装置であって、(a) 前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するよう、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、

前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを備えることを特徴とする。

前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付け手段と、1つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段と、前記暗号化鍵特定手段により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成する暗号化手段と、前記暗号化手段により生成された暗号化配給用データ群を外部に出力する出力手段とを備えることを特徴とする。

【0163】また、本発明に係る暗号化鍵特定方法は、3台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定するための暗号化鍵特定方法であって、前記各端末が、2つ以上の端末を要素に含む集合である端末集合の少なくとも1つには属するように、更に、同じ1つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、2つ以上の端末集合を決定する端末集合決定ステップと、端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、1つ以上の端末を無効化端末として特定する無効化端末特定ステップと、前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とする。

【0164】これらにより、例えば、各端末へ記録媒体に暗号化された結果のデータを記録して記録媒体を配布する場合において、暗号化に用いる暗号化鍵の数を比較

的少なく抑えることができるので、その記録媒体に記録されるデータの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合にその特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるように、その暗号化を実施することが可能になる。

【図面の簡単な説明】

【図1】本発明の実施の形態1に係るデータ保護システム100の概略構成図である。

10 【図2】暗号化装置101及び復号装置103aの機能構成図である。

【図3】鍵設定システム104の機能構成図である。

【図4】4分木の木構造を示す図である。

【図5】復号装置数が64台である場合における4分木の木構造の例を示す図である。

【図6】ルートの無効化情報の例を示す図である。

【図7】ルートの無効化情報の例を示す図である。

【図8】4分木の木構造のレベル0及びレベル1の階層のノードに対応して割り当てる鍵を示す図である。

20 【図9】鍵情報格納部301に格納される鍵情報の構成を示す図である。

【図10】復号鍵決定部305により実行される鍵割当処理を示すフローチャートである。

【図11】64台しか復号装置がないと仮定した場合においてレベル3の相対番号1のリーフに対応する復号装置(端末1)に割り当てるものと鍵割当処理によって決定される復号鍵群905を示す図である。

【図12】鍵情報更新部304により実行される無効化情報更新処理を示すフローチャートである。

30 【図13】暗号化鍵特定部306により実行される鍵特定処理を示すフローチャートである。

【図14】64台しか復号装置がないと仮定した場合において、無効化端末がない状態での暗号化鍵等を示す図である。

【図15】64台しか復号装置がないと仮定した場合において、端末1が無効化端末である状態での暗号化鍵等を示す図である。

【図16】図15に示す暗号化鍵に対応する鍵特定情報の一例を示す図である。

40 【図17】実施の形態2に係る第2データ保護システムにおいて復号装置数が64台である場合に構築される4つの4分木の木構造の例を示す図である。

【図18】第2データ保護システムにおいて、端末1が無効化端末である状態での暗号化鍵等を示す図である。

【図19】実施の形態3において用いられる4分木の木構造における各ノードに割り当てる復号鍵を示す図である。

50 【図20】64台しか復号装置がないと仮定した場合においてレベル3の相対番号1のリーフに対応する復号装置(端末1)に割り当てる復号鍵群1705を示す

図である。

【図21】64台しか復号装置がないと仮定した場合において、端末1、端末2及び端末17が無効化端末である状態での暗号化鍵等を示す図である。

【図22】本発明の実施の形態4に係る第4データ保護システムの概略構成図である。

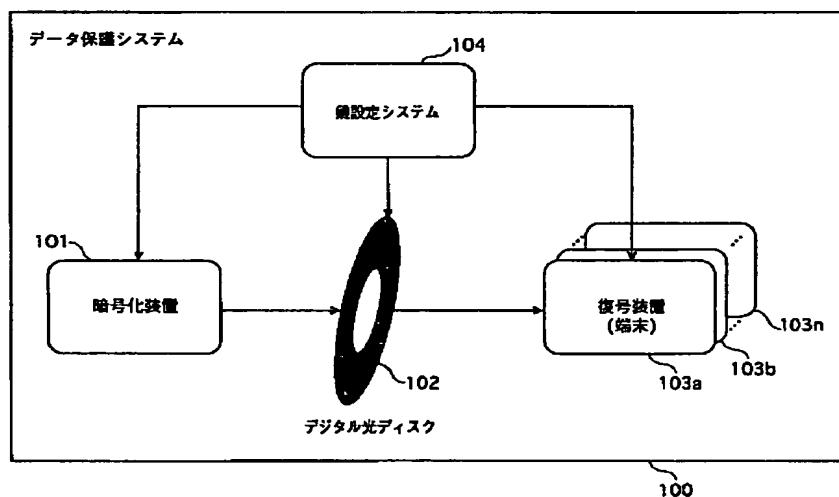
【符号の説明】

100 データ保護システム
101 暗号化装置
102 光ディスク
103a～103n 復号装置
104 鍵設定システム
201 コンテンツ記憶部
202 乱数発生部
203 暗号化鍵群格納部
204 鍵暗号化部

* 205 コンテンツ暗号化部
206 出力部
211 取得部
212 復号鍵群格納部
213 復号鍵選定部
214 鍵復号部
215 コンテンツ復号部
216 再生部
301 鍵情報格納部
10 302 鍵情報生成部
303 無効化端末特定部
304 鍵情報更新部
305 復号鍵決定部
306 暗号化鍵特定部
1501 鍵特定情報記録装置
* 1502a～1502n ユーザデータ暗号化装置

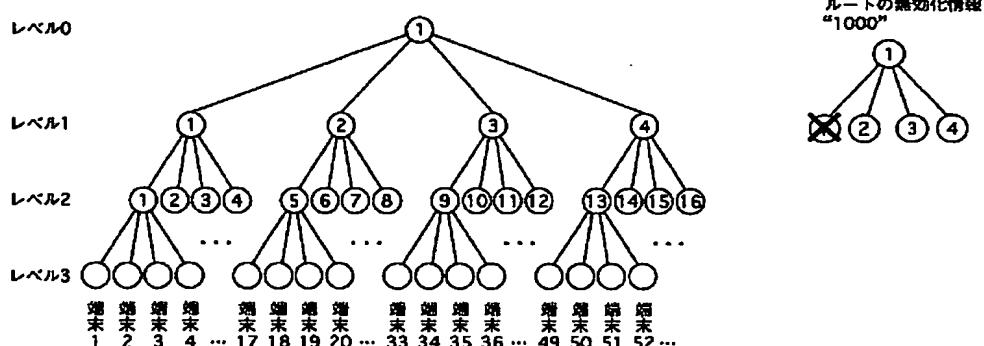
【図1】

【図6】

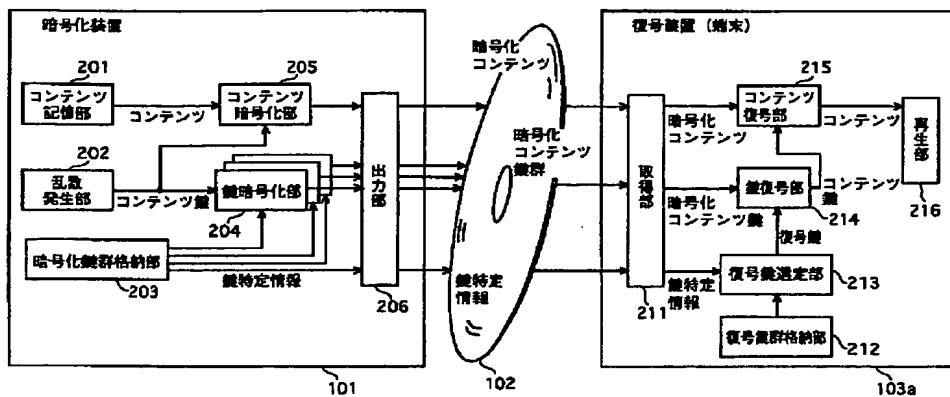


【図5】

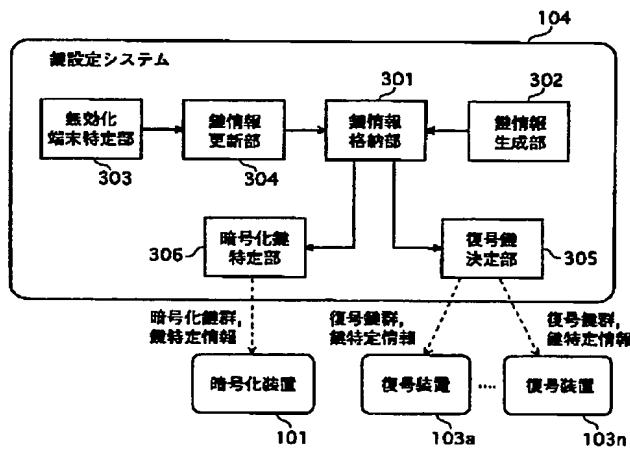
【図7】



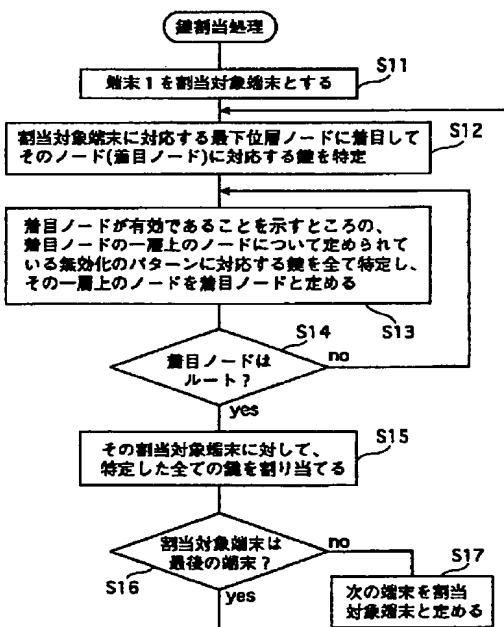
【図2】



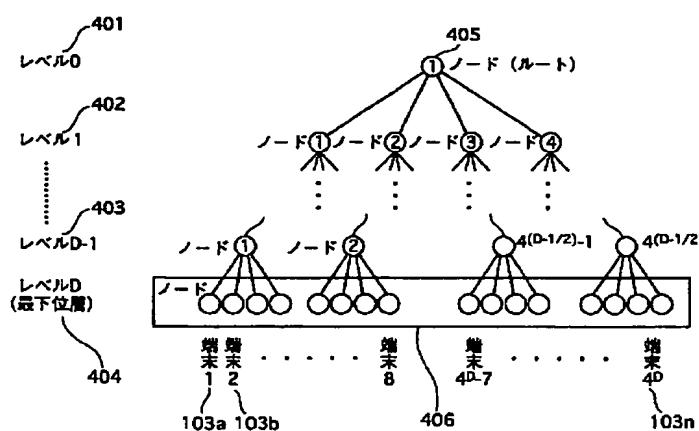
【図3】



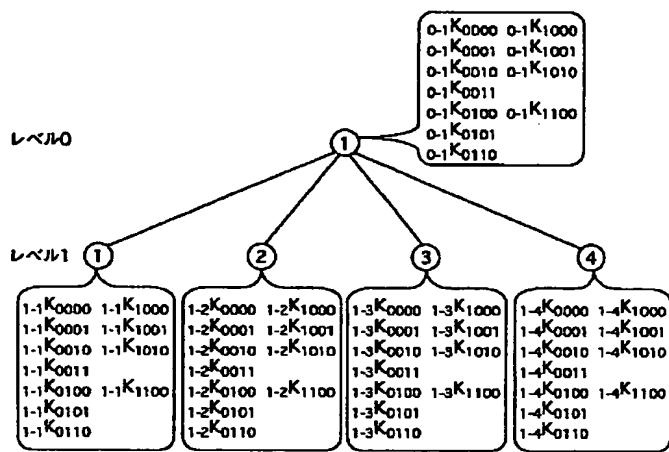
【図 10】



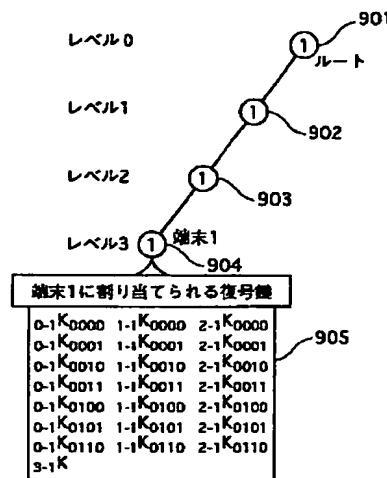
〔四〕



【図8】



【図11】

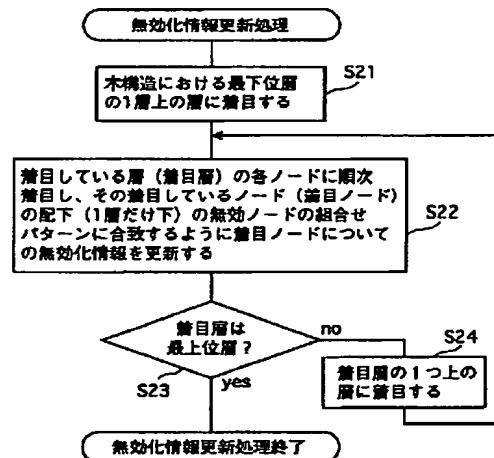


【図9】

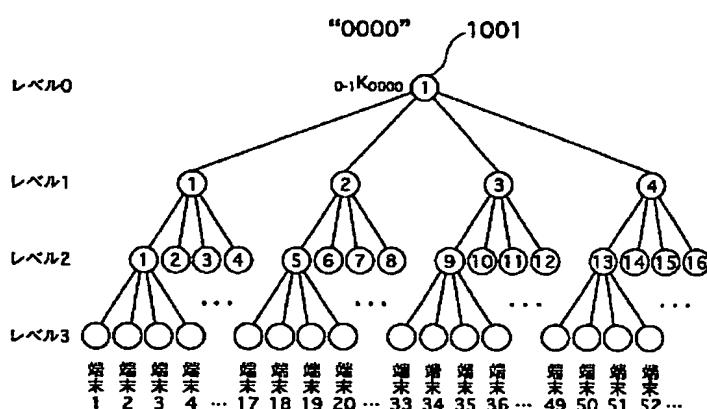
500 錯情報

ノードID	無効化パターン	端	無効化情報
0-1	0000	0-1K0000	0000
	0001	0-1K0001	
	0010	0-1K0010	
	0011	0-1K0011	
	0100	0-1K0100	
	0101	0-1K0101	
	0110	0-1K0110	
	1000	0-1K1000	
	1001	0-1K1001	
	1010	0-1K1010	
1-1	0000	1-1K0000	0000
	0001	1-1K0001	
	0010	1-1K0010	
	0011		

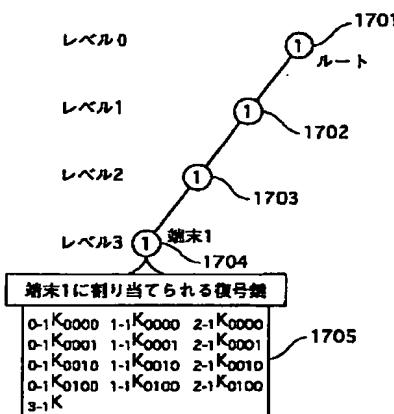
【図12】



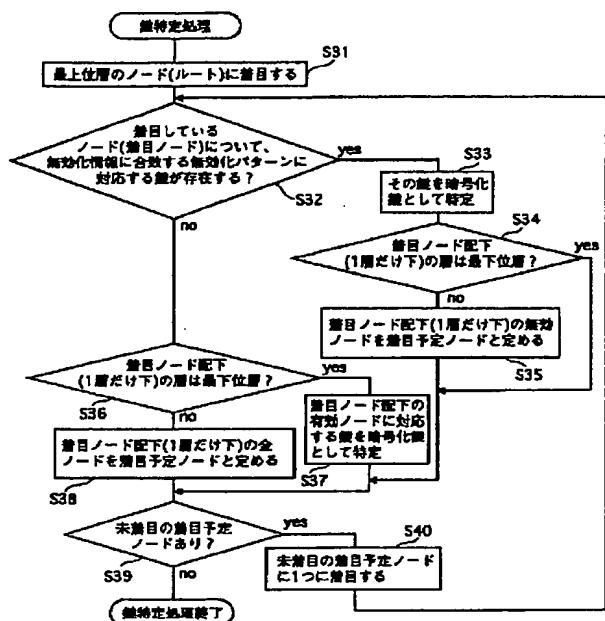
【図14】



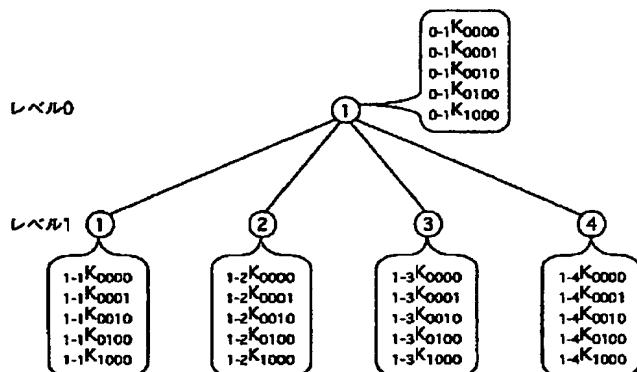
【図20】



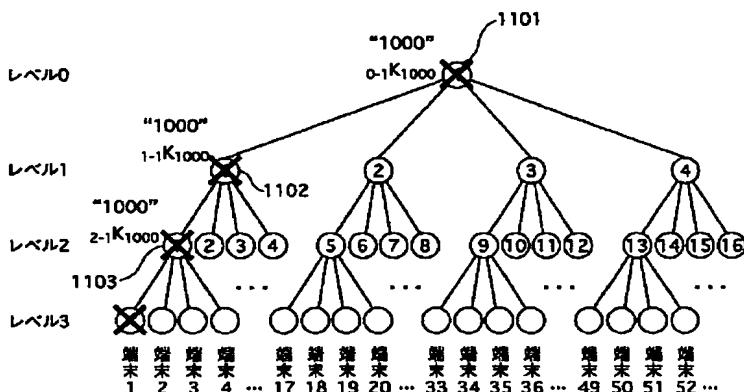
【図13】



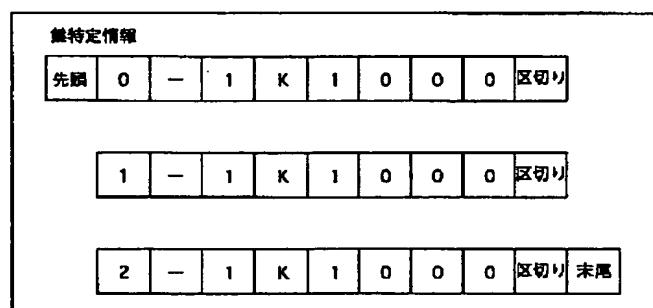
【図19】



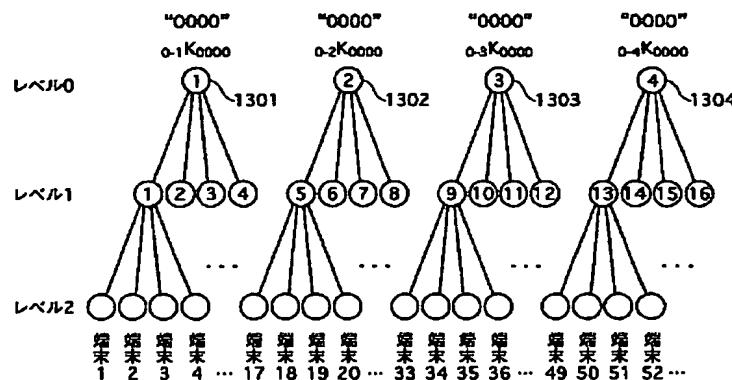
【図15】



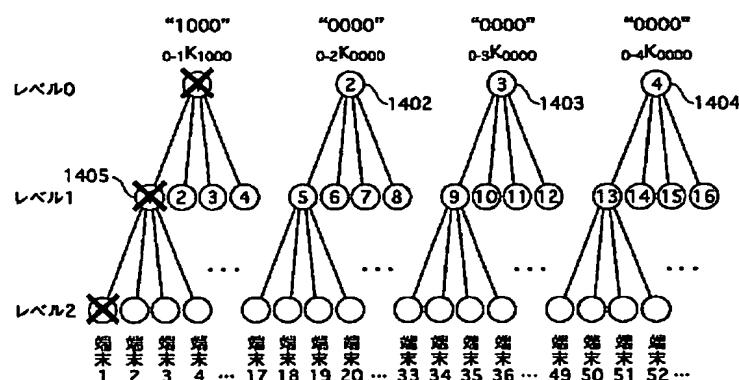
【図16】



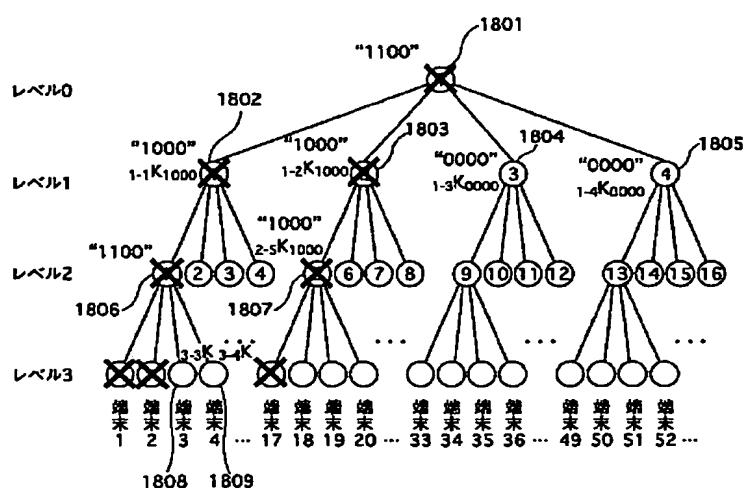
【図17】



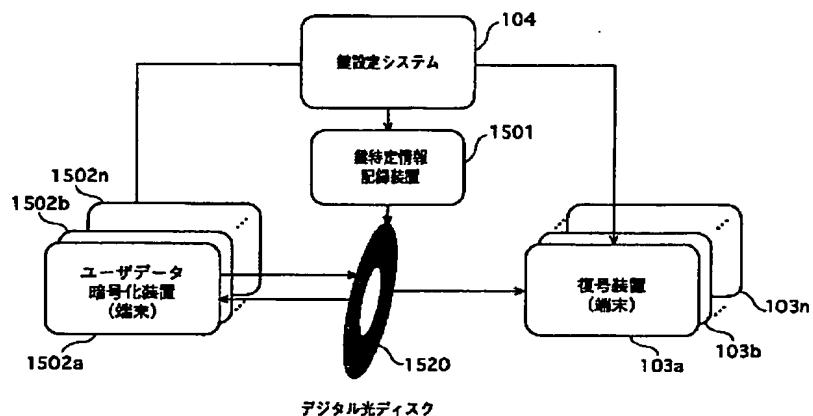
【図18】



【図21】



【図22】



フロントページの続き

(72)発明者 松崎 なつめ
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 館林 誠
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

F ターム(参考) 5C053 FA13 FA24 GB40
5D044 BC02 CC04 DE50 EF05 FG18
GK12 GK17 GK20

5J104 AA12 AA16 EA04 MA05 NA02
NA27

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (usptf)